

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN")

WHITNEY LILIANA ACOSTA ROBELTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA DC
2019

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN”)

WHITNEY LILIANA ACOSTA ROBELTO

Trabajo presentado como requisito para optar al título de Ingeniero de Sistemas.

Director de diplomado de profundización: JUAN CARLOS VESGA

Tutor: EFRAÍN ALEJANDRO PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
INGENIERIA DE SISTEMAS

BOGOTA DC

2019

Nota de aceptación

Firma del presidente del Jurado

Firma del jurado

Bogotá, 12 de Diciembre de 2019

DEDICATORIA

Dedico este trabajo primeramente a Dios, que gracias a su sabiduría e Inteligencia otorgada, pude desarrollar mis destrezas y habilidades en el camino de la Ingeniería de Sistemas.

A mi familia quienes siempre estuvieron a mi lado apoyándome y por qué gracias a ellos tuve las fuerzas para continuar adelante. En especial a mi madre Lilia Robelto por su amor y apoyo incondicional que me ha dado, a ella le dedico este triunfo con todo el amor del mundo.

AGRADECIMIENTOS

Agradezco a Dios por permitirme la vida, permitirme crecer personalmente y laboralmente, siendo él mi apoyo y fortaleza en los momentos de debilidad.

Agradezco a la Universidad Nacional Abierta y a Distancia por permitirme ser una de sus estudiantes para la Escuela de Ciencias Básicas Tecnología e Ingeniería, dándome la oportunidad crecer profesionalmente y permitirme alcanzar mis metas.

RESUMEN

El presente trabajo es un desarrollo de habilidades prácticas que trata sobre la puesta en marcha de nuestros conocimientos frente a las redes de telecomunicaciones, basándonos en los módulos de cisco en los que se recopiló información teórica necesaria, el cual nos permite realizar un buen diagnóstico y comprensión del desarrollo de actividades sobre los requerimientos propuestos.

Así mismo este trabajo final concierne a la prueba de habilidades prácticas del Diplomado de Profundización Cisco, cursado en la Universidad Nacional Abierta y a Distancia en convenio con la plataforma de Cisco.

ABSTRACT

This document is a development of practical skills that deals with the implementation of our knowledge in front of telecommunications networks, based on cisco modules in which necessary theoretical information is collected which allows us to make a good diagnosis and understanding of the development of activities on the proposed requirements.

Likewise, this final concierge work to the practical skills test of the Cisco Deepening Diploma, studied at Universidad Nacional Abierta y a Distancia in agreement with the Cisco platform.

TABLA DE CONTENIDO

0. INTRODUCCIÓN	1
1. OBJETIVOS GENERALES.....	2
2. OBJETIVOS ESPECIFICOS.....	3
3. DESCRIPCIÓN DE ESCENARIO 1	4
4. ASIGNACIÓN DE LOS NOMBRES.....	5
5. ASIGNACIÓN DE CLAVES DE SEGURIDAD	7
6. CONEXIONES FISICAS PARA LA TOPOLOGIA DE RED.....	9
7. CONFIGURACIÓN DE LA TOPOLOGÍA DE RED	10
7.1 SUBNETING PARA 8 SEGMENTOS DE RED	10
8. TABLA DE DIRECCIONAMIENTO DE RED.....	11
9. CONFIGURACIÓN DE LOS ROUTER	12
10. VERIFICACIÓN DE LA TABLA DE ENRUTAMIENTO PARA ROUTER.....	15
11. DIAGNOSTICO DE VECINDAD BAJO EL PROTOCOLO CDP	17
12. PRUEBAS DE CONECTIVIDAD DESDE CADA TRAMO BAJO EL COMANDO PING	19
13. CONFIGURACION DE ENRUTAMIENTO.....	21
14. VERIFICACIÓN DE RUTAS ESTABLECIDAS EN LOS ROUTER	24
15. DIAGNOSTICO DE CONECTIVIDAD ENTRE SEDES MEDELLIN. BOGOTA Y CALI	27
16. CONFIGURACIÓN DE LISTAS DE CONTROL DE ACCESO	30
17. CONFIGURACIÓN PARA QUE SOLO EL SERVIDOR TENGA ACCESO A CUALQUIER DISPOSITIVO DE LA RED.....	32
18. CONFIGURACIÓN DE LA LAN DE MEDELLIN Y CALI PARA DENEGAR TRÁFICO A CUALQUIER OTRO DISPOSITIVO EN CUALQUIER PARTE DE LA RED	33
19. COMPROBAR LA RED INSTALADA	34
20. COMPLETAR LA SIGUIENTE TABLA DE CONDICIONES DE PRUEBA PARA CONFIRMAR EL ÓPTIMO FUNCIONAMIENTO DE LA RED	39

21. DESCRIPCIÓN DE ESCENARIO 2	40
22. CONFIGURACIÓN BÁSICA EN LOS ROUTER	41
23. CONFIGURACIÓN DE INTERFACES	51
23.1 CONFIGURACIÓN DE INTERFACES	53
23.2 ACTIVACIÓN DE VLANS EN SWITCH	60
23.3 CONFIGURACIÓN DESCRIPCIÓN DE LAS INTERFACES	64
24. ENRUTAMIENTO OSPF CON AUTENTICACIÓN	67
25. AUTENTICACIÓN LOCAL CON AAA	71
26. MAXIMO DE INTENTOS PARA ACCEDER AL ROUTER Y TIEMPO DE INGRESO	75
27. CONFIGURACIÓN DE SERVIDOR TFTP PARA ALMACENAMIENTO DE ARCHIVOS EN LOS ROUTER.....	77
28. CONFIGURACIÓN DE DHCP PARA BUCARAMANGA Y CUNDINAMARCA CON IP HELPER-ADDRESS DESDE TUNJA	79
29. HABILITAR OPCIONES EN PUERTO DE CONSOLA Y TERMINAL VIRTUAL	84
30. CONFIGURACIÓN DE NAT ESTATICO PARA EL WEB SERVER Y SOBRECARGA PAT	87
31. SOBRECARGA PAT PARA LOS DEMÁS EQUIPOS	89
32. ESTABLECER ACL PARA EL ESCENARIO 2	90
32.1 Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.	90
32.2 Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.	93
32.3 Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10	95
32.4 Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.....	97
32.5 Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.	99
32.6 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.....	100

33. CONCLUSIONES	101
34. BIBLIOGRAFIA	102

LISTA DE FIGURAS

Figura 1. Escenario 1	4
Figura 2. Topología para el escenario 1	9
Figura 3. Tabla de enrutamiento router Medellín	15
Figura 4. Tabla de enrutamiento router Bogota.....	16
Figura 5. Tabla de enrutamiento router Cali.....	16
Figura 6. Vecindad en el router Medellín a través de CDP	17
Figura 7. Vecindad en el router Bogota a través de CDP	18
Figura 8. Vecindad en el router Cali a través de CDP.....	18
Figura 9. Prueba de ping a sede Medellín.....	19
Figura 10. Prueba de ping a sede Bogota.....	19
Figura 11. Prueba de ping a sede Cali	20
Figura 12. Prueba de ping a sede Bogota.....	20
Figura 13. Tabla de enrutamiento Medellín	23
Figura 14. Tabla de enrutamiento Bogota	23
Figura 15. Tabla de enrutamiento Cali.....	23
Figura 16. Tabla de enrutamiento Medellín	24
Figura 17. Tabla de enrutamiento Bogota	25
Figura 18. Tabla de enrutamiento Bogota	26
Figura 19. Configuración de host de diferente LAN	27
Figura 20. Prueba ICMP desde host de la LAN de Cali a host en la LAN de Medellín	28
Figura 21. Configuración de host de diferente LAN	28
Figura 22. Prueba ICMP desde host de la LAN de Cali hacia el servidor	29
Figura 23. Prueba ICMP desde host de la LAN de Cali hacia el servidor	34
Figura 26. Acceso al servidor desde la LAN PC1-Cali	36
Figura 28. Prueba ICMP desde host de la LAN de Medellín hacia Cali.	37
Figura 30. Acceso al servidor desde PC1_Medellín	38

Figura 31. Escenario 2	40
Figura 32. Configuración OSPF con autenticación para Bucaramanga	68
Figura 33. Configuración OSPF con autenticación para Tunja	69
Figura 34. Configuración OSPF con autenticación para Cundinamarca	70
Figura 35. Direccionamiento IP por DHCP desde el router de Tunja	81
Figura 36. Direccionamiento IP por DHCP desde el router de Bucaramanga	83
Figura 37. Configuración NAT estático para Web Server Interno	88
Figura 38. Configuración NAT estático para Web Server Externo.....	88
Figura 39. Configuración PAT de sobrecarga.....	89
Figura 40. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja.	91
Figura 41. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja.....	91
Figura 42. Ping desde PC Cundinamarca hacia Internet.	92
Figura 43. Ping desde PC Tunja VLAN 20 a PC Cundinamarca VLAN 20.....	94
Figura 44. Ping desde PC Tunja VLAN 20 a PC Bucaramanga VLAN 10	94
Figura 45. Ping desde PC Bucaramanga VLAN 30 hacia VLAN 10 PC Bucaramanga	96
Figura 46. Ping desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Tunja ...	98
Figura 47. Ping desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Cundinamarca	98

0. INTRODUCCIÓN

En la actualidad las empresas de telecomunicaciones requieren de actualizaciones tecnológicas y estructurales para sus áreas e inclusive ciudades. Es por ello que para este trabajo se aplican conocimientos adquiridos en el diplomado de profundización CCNA, en el cual a través de la prueba de habilidades prácticas nos permite desarrollar la implementación de una red WAN/LAN en la que podemos realizar desde configuraciones básicas, enrutamientos a través de protocolos como OSPFv3 y EIGRP, así mismo ACL que nos permite el acceso de tráfico para algunas redes, y así mismo para denegar.

Por lo tanto el desarrollo del presente trabajo nos permitirá fortalecer nuestros conocimientos y habilidades para futuros desarrollos en ambientes reales.

1. OBJETIVOS GENERALES

El objetivo principal de este trabajo es desarrollar la implementación de dos escenarios de red a nivel WAN/LAN, cumpliendo los requerimientos suministrados en la prueba de habilidades prácticas del CCNA, enfocado en habilidades de destreza para el aprendizaje personal y profesional.

2. OBJETIVOS ESPECIFICOS

- Incluir en el desarrollo de la red configuraciones básicas para cada uno de los equipos como Router y Switch.
- Identificar posibles errores en la red y dar solución a través de Troubleshooting para obtener un mejor funcionamiento en la red.
- Permitir escalabilidad de la red sobre el escenario 1, para redes futuras.
- Comprobar el funcionamiento correcto en cada uno de los escenarios propuestos a través de trazas y pruebas ICMP.

3. DESCRIPCIÓN DE ESCENARIO 1

Escenario 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

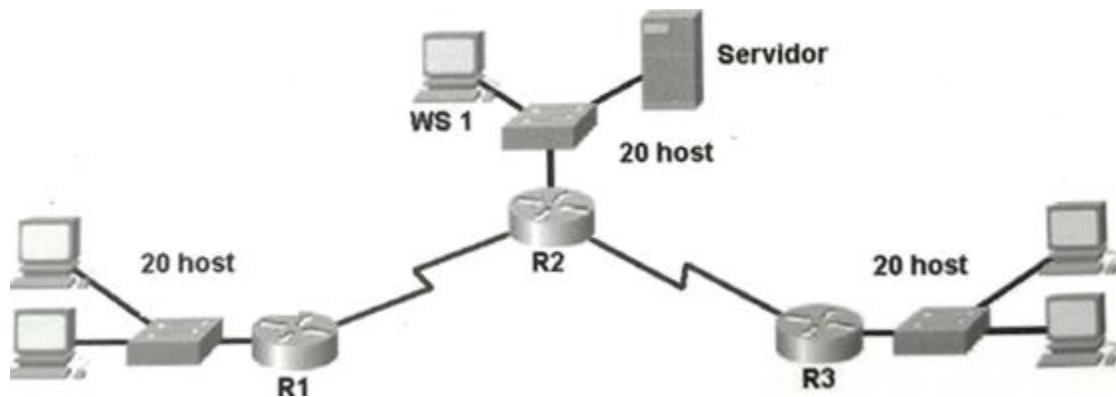


Figura 1. Escenario 1

4. ASIGNACIÓN DE LOS NOMBRES

Se asignan respectivos nombres a los Routers de acuerdo a las sedes estipuladas.

Router Medellín

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config) #hostname MEDELLIN
MEDELLIN (config) #do wr
Building configuration...
[OK]
MEDELLIN (config) #end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN#
```

Router Bogota

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config) #hostname BOGOTA
BOGOTA (config) #do wr
Building configuration...
[OK]
BOGOTA(config)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA#
```

Router Cali

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname CALI

CALI(config)#do wr

Building configuration...

[OK]

CALI(config)#end

CALI#

%SYS-5-CONFIG_I: Configured from console by console

CALI#

5. ASIGNACIÓN DE CLAVES DE SEGURIDAD

Se procede a realizar asignación de contraseñas para los router Medellín, Bogota y Cali, de esta manera; para enable cisco y para la línea de consola class.

Se usan los siguientes comandos

Router Medellín

```
MEDELLIN>enable
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#enable password cisco
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password class
MEDELLIN(config-line)#login
MEDELLIN(config-line)#do wr
Building configuration...
[OK]
MEDELLIN(config-line)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN#
```

Router Bogota

```
BOGOTA>enable
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#enable password cisco
BOGOTA(config)#line console 0
BOGOTA(config-line)#password class
BOGOTA(config-line)#login
BOGOTA(config-line)#do wr
Building configuration...
[OK]
BOGOTA(config-line)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
```

Router Cali

```
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#enable password cisco
CALI(config)#line console 0
CALI(config-line)#password class
CALI(config-line)#login
CALI(config-line)#
CALI(config-line)#do wr
Building configuration...
[OK]
CALI(config-line)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console

CALI#
```

6. CONEXIONES FISICAS PARA LA TOPOLOGIA DE RED

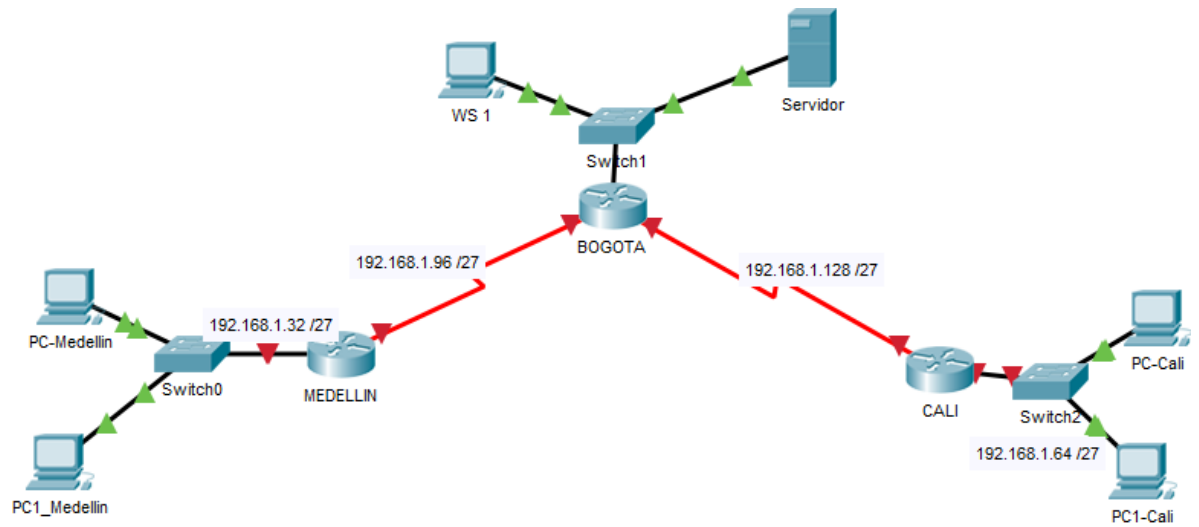


Figura 2. Topología para el escenario 1

7. CONFIGURACIÓN DE LA TOPOLOGÍA DE RED

En este espacio damos como inicio al proceso de Subneting para las redes del escenario 1, en el que se debe dividir la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.

7.1 SUBNETING PARA 8 SEGMENTOS DE RED

DIRECCIÓN	MASCARA	HOST UTILIZABLES	BROADCAST
192.168.1.0 /27	255.255.255.224	192.168.1.1 – 192.168.1.30	192.168.1.31
192.168.1.32 /27	255.255.255.224	192.168.1.33 – 192.168.1.62	192.168.1.63
192.168.1.64 /27	255.255.255.224	192.168.1.65 – 192.168.1.94	192.168.1.95
192.168.1.96 /27	255.255.255.224	192.168.1.97 – 192.168.1.126	192.168.1.127
192.168.1.128 /27	255.255.255.224	192.168.1.129 – 192.168.1.158	192.168.1.159
192.168.1.160 /27	255.255.255.224	192.168.1.161 – 192.168.1.190	192.168.1.191
192.168.1.192 /27	255.255.255.224	192.168.1.193 – 192.168.1.222	192.168.1.223

192.168.1.224 /27	255.255.255.224	192.168.1.225 – 192.168.1.254	192.168.1.255
-------------------	-----------------	----------------------------------	---------------

Tabla 1. Segmentos de red

A continuación se completara la siguiente tabla con la configuración básica de los router, teniendo en cuenta las subredes diseñadas anteriormente.

8. TABLA DE DIRECCIONAMIENTO DE RED

	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	192.168.1.162	192.168.1.130	192.168.1.194
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	EIGRP	EIGRP	EIGRP
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Tabla 2. Direccionamiento de red escenario 1.

9. CONFIGURACIÓN DE LOS ROUTER

Router Medellín

Se realiza configuración para las interfaces serial 0/0/0, serial 0/0/1 y Fastethernet 0/0 sobre el router de Medellín

```
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface serial 0/0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN(config-if)#interface serial 0/0/1
MEDELLIN(config-if)#ip address 192.168.1.162 255.255.255.224
MEDELLIN(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
MEDELLIN(config-if)#interface Fa0/1
MEDELLIN(config-if)#no ip address
MEDELLIN(config-if)#interface giga0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
MEDELLIN(config-if)#do wr
Building configuration...
[OK]
MEDELLIN(config-if)#
```

Router Bogota

Se realiza configuración para las interfaces serial 0/0/0, serial 0/0/1 y Fastethernet 0/0 sobre el router de Bogota

```
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#interface serial 0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
```



```

BOGOTA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

BOGOTA(config-if)#interface serial 0/0/
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA(config-if)#interface g0/1
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
BOGOTA(config-if)#do wr
Building configuration...
[OK]
BOGOTA(config-if)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

```

Router Cali

Se realiza configuración para las interfaces serial 0/0/0, serial 0/0/1 y Fastethernet 0/0 sobre el router de Cali

```

CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#interface serial 0/0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
CALI(config-if)#

```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
CALI(config-if)#interface serial0/0/1
CALI(config-if)#ip address 192.168.1.194 255.255.255.224
CALI(config-if)#no shu
CALI(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
CALI(config-if)#
CALI(config-if)#interface g0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
CALI(config-if)#do wr
Building configuration...
[OK]
CALI(config-if)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
```

10. VERIFICACIÓN DE LA TABLA DE ENRUTAMIENTO PARA CADA ROUTER

Se procede a verificar la tabla de enrutamiento sobre cada uno de los equipos de las sedes: Medellín, Cali y Bogotá.

MEDELLIN

Show ip route

```
MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2, O - OSPF other
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0

MEDELLIN#
```

Figura 3. Tabla de enrutamiento router Medellín

BOGOTA

Show ip route

```
BOGOTA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external t
        E1 - OSPF external type 1, E2 - OSPF external type 2, E -
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.130/32 is directly connected, Serial0/0/1

BOGOTA#
```

Figura 4. Tabla de enrutamiento router Bogota

CALI

Show ip route

```
CALI#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mol
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF i
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA extern
        E1 - OSPF external type 1, E2 - OSPF external type 2,
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
inter area
        * - candidate default, U - per-user static route, o -
        P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 mask:
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.131/32 is directly connected, Serial0/0/0

CALI#
```

Figura 5. Tabla de enrutamiento router Cali

11. DIAGNOSTICO DE VECINDAD BAJO EL PROTOCOLO CDP

El diagnostico se realizó bajo el comando CDP el cual nos permite obtener información del router y de su vecindad que estén conectados localmente. Para ello se procede con la activación del comando sobre los router: Medellín, Bogota y Cali

Router Medellin

```
MEDELLIN(config)#cdp run
MEDELLIN(config)#do wr
Building configuration...
[OK]
MEDELLIN(config)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#
```

```
MEDELLIN# sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme  Capability  Platform  Port ID
Switch           Gig 0/1         133      S           2960      Fas 0/2
BOGOTA           Ser 0/0/0       170      R           C1900     Ser 0/0/0
MEDELLIN#
```

Figura 6. Vecindad en el router Medellín a través de CDP

Router Bogota

```
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#cdp run
BOGOTA(config)#do wr
Building configuration...
[OK]
BOGOTA(config)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by
```

```

BOGOTA#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme  Capability  Platform  Port ID
Switch           Gig 0/1        140      S           2960      Fas 0/2
CALI              Ser 0/0/1        140      R           C1900     Ser 0/0/0
MEDELLIN         Ser 0/0/0        140      R           C1900     Ser 0/0/0
BOGOTA#

```

Figura 7. Vecindad en el router Bogota a través de CDP

Router Cali

```

CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#cdp run
CALI(config)#do wr
Building configuration...
[OK]
CALI(config)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#

```

```

CALI#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme  Capability  Platform  Port ID
BOGOTA           Ser 0/0/0        167      R           C1900     Ser 0/0/1
CALI#

```

Figura 8. Vecindad en el router Cali a través de CDP

12. PRUEBAS DE CONECTIVIDAD DESDE CADA TRAMO BAJO EL COMANDO PING

Realizamos prueba ICMP desde la WAN del router Bogota a la WAN del router Medellín, para comprobar conectividad en las configuraciones realizadas sobre cada tramo.

PRUEBA DE PING DESDE BOGOTA A MEDELLIN

```
BOGOTA#ping 192.168.1.98
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/12/52 ms
```

Figura 9. Prueba de ping a sede Medellín

PRUEBA DE PING DESDE MEDELLIN A BOGOTA

```
MEDELLIN#ping 192.168.1.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/7/25
MEDELLIN#
```

Figura 10. Prueba de ping a sede Bogota

PRUEBA DE PING DESDE BOGOTA A CALI

```
BOGOTA#ping 192.168.1.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
BOGOTA#
```

Figura 11. Prueba de ping a sede Cali

PRUEBA DE PING DESDE CALI A BOGOTA

```
CALI#ping 192.168.1.130
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/32 ms
```

Figura 12. Prueba de ping a sede Bogota

13.CONFIGURACION DE ENRUTAMIENTO

Realizamos la configuración de enrutamiento en las redes bajo el protocolo EIGRP acompañado del sistema autónomo 200, esta configuración se realiza para cada una de las sedes; Medellín, Bogota y Cali.

Para este enrutamiento usamos el protocolo EIGRP el cual mantiene el algoritmo vector distancia y la información de la métrica original del protocolo IGRP.

Así mismo este protocolo es de transporte fiable ya que este garantiza la entrega correcta y ordenada de información, manteniendo las actualizaciones que se generen en la tabla de enrutamiento.

Para realizar la configuración sobre cada uno de los router de las sedes mencionadas se realizo el siguiente procedimiento:

MEDELLIN(config)#router eigrp 200

MEDELLINconfig-router)#network 192.168.1.99 0.0.0.224

ENRUTAMIENTO EIGRP ROUTER MEDELLÍN

```
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#network 192.168.1.33 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.99 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.162 0.0.0.31
MEDELLIN(config-router)#do wr
Building configuration...
[OK]
MEDELLIN(config-router)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN
```

ENRUTAMIENTO EIGRP ROUTER BOGOTA

```

BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#network 192.168.1.1 0.0.0.31
BOGOTA(config-router)#network 192.168.1.98 0.0.0.31
BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0/0) is
up: new adjacency
BOGOTA(config-router)#network 192.168.1.130 0.0.0.31
BOGOTA(config-router)#do wr
Building configuration...
[OK]
BOGOTA(config-router)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#

```

ENRUTAMIENTO EIGRP ROUTER CALI

```

CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 200
CALI(config-router)#no auto-summary
CALI(config-router)#network 192.168.1.65 0.0.0.31
CALI(config-router)#network 192.168.1.131 0.0.0.31
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is
up: new adjacency
CALI(config-router)#network 192.168.1.194 0.0.0.31
CALI(config-router)#do wr
Building configuration...
[OK]
CALI(config-router)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#

```

VERIFICACIÓN DE VECINDAD EN LOS ROUTER CON EIGRP

Se usó el comando `show ip eigrp neighbors` para conocer la vecindad en las sedes Bogota, Medellín desde Cali y viceversa. Este comando permite verificar el enrutamiento realizado de manera adecuada.

MEDELLÍN

```
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address          Interface      Hold Uptime    SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt   Num
0   192.168.1.98      Se0/0/0       11  00:16:39    40    1000   0   5
MEDELLIN#
```

Figura 13. Tabla de enrutamiento Medellín

BOGOTA

```
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address          Interface      Hold Uptime    SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt   Num
0   192.168.1.99      Se0/0/0       13  00:24:07    40    1000   0   7
1   192.168.1.131     Se0/0/1       12  00:14:13    40    1000   0   5
BOGOTA#
```

Figura 14. Tabla de enrutamiento Bogota

CALI

```
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address          Interface      Hold Uptime    SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt   Num
0   192.168.1.130     Se0/0/0       13  00:14:52    40    1000   0   6
CALI#
```

Figura 15. Tabla de enrutamiento Cali

14. VERIFICACIÓN DE RUTAS ESTABLECIDAS EN LOS ROUTER

Bajo el enrutamiento realizado con el protocolo EIGRP, en este espacio se verificaran las rutas establecidas en los router de las sedes Medellín, Bogotá y Cali.

Para ello se usó el comando show ip route

TABLA DE ENRUTAMIENTO MEDELLÍN

```
MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:31:29, Serial0/0/0
D       192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:21:35, Serial0/0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:31:19, Serial0/0/0

MEDELLIN#
```

Figura 16. Tabla de enrutamiento Medellín

TABLA DE ENRUTAMIENTO BOGOTA

```
BOGOTA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
D       192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:30:14,
Serial0/0/1
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.130/32 is directly connected, Serial0/0/1

BOGOTA#
```

Figura 17. Tabla de enrutamiento Bogota

TABLA DE ENRUTAMIENTO CALI

```
CALI#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

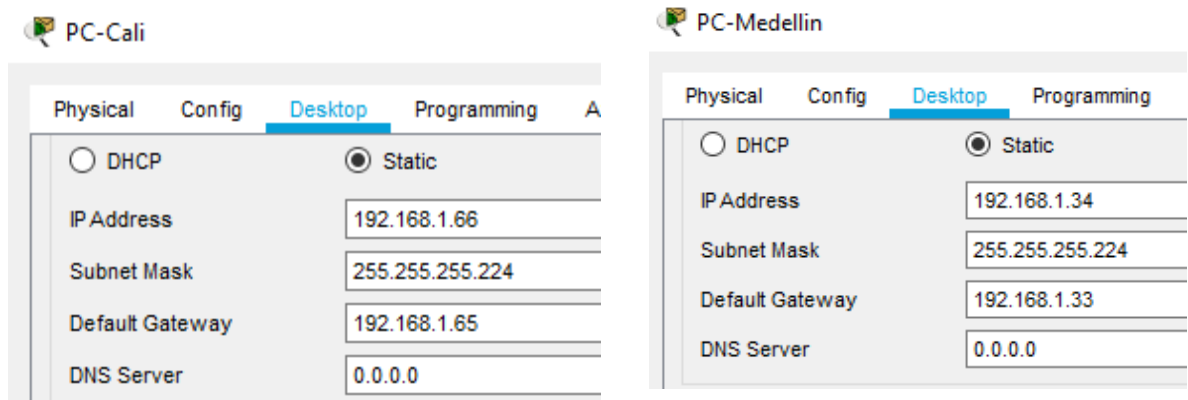
    192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.130, 00:32:40, Serial0/0/0
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:32:40,
Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.131/32 is directly connected, Serial0/0/0
CALI#
```

Figura 18. Tabla de enrutamiento Bogota

15. DIAGNOSTICO DE CONECTIVIDAD ENTRE SEDES MEDELLIN. BOGOTA Y CALI

Se realiza prueba ICMP de conectividad entre las sedes, luego de realizar enrutamiento EIGRP.

PING DESDE PC-CALI A PC_MEDELLIN



The image displays two side-by-side screenshots of network configuration interfaces for two PCs: PC-Cali and PC-Medellin. Both interfaces show the 'Desktop' tab selected, indicating static IP configurations.

PC-Cali Configuration:

Field	Value
IP Address	192.168.1.66
Subnet Mask	255.255.255.224
Default Gateway	192.168.1.65
DNS Server	0.0.0.0

PC-Medellin Configuration:

Field	Value
IP Address	192.168.1.34
Subnet Mask	255.255.255.224
Default Gateway	192.168.1.33
DNS Server	0.0.0.0

Figura 19. Configuración de host de diferente LAN

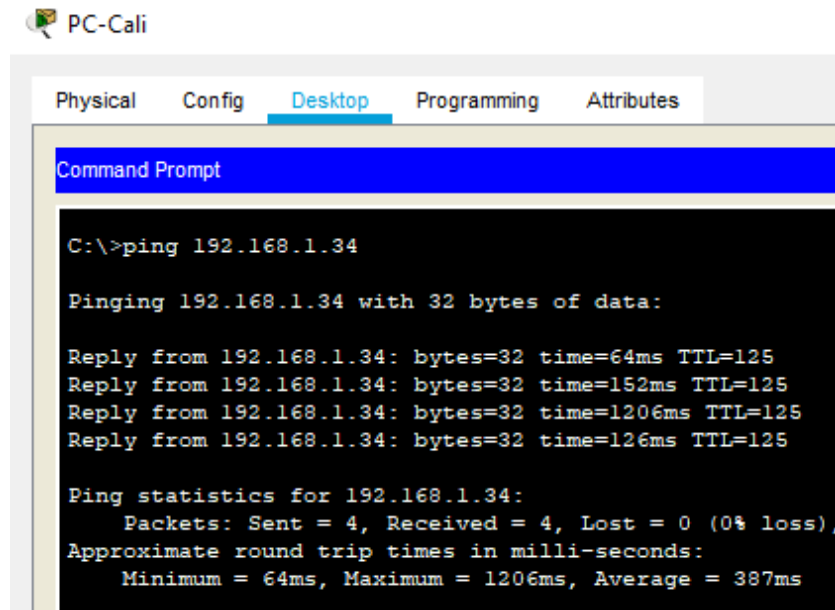


Figura 20. Prueba ICMP desde host de la LAN de Cali a host en la LAN de Medellín

PING DESDE PC1-CALI A SERVIDOR

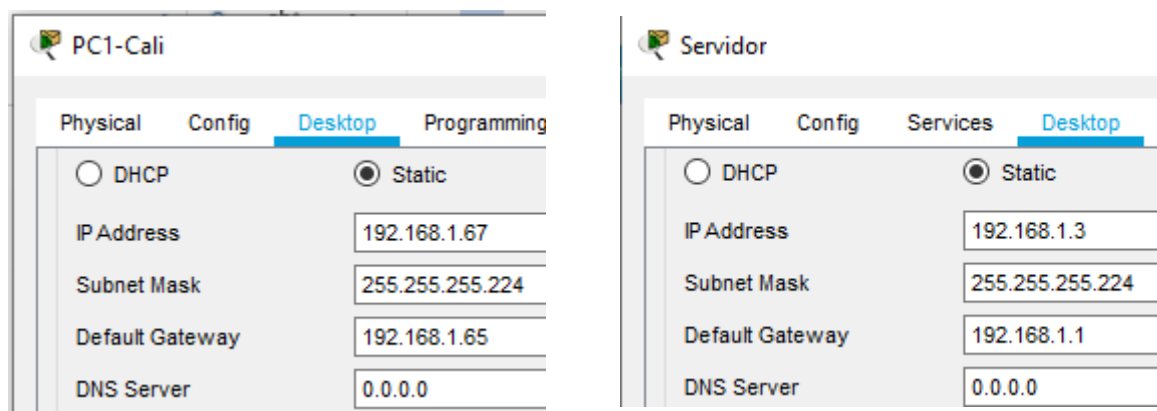
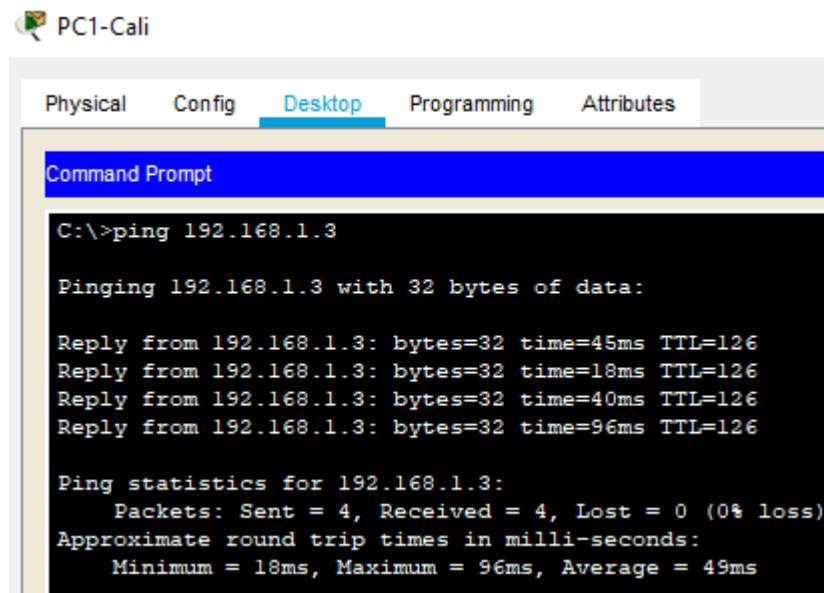


Figura 21. Configuración de host de diferente LAN



```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=45ms TTL=126
Reply from 192.168.1.3: bytes=32 time=18ms TTL=126
Reply from 192.168.1.3: bytes=32 time=40ms TTL=126
Reply from 192.168.1.3: bytes=32 time=96ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 96ms, Average = 49ms
```

Figura 22. Prueba ICMP desde host de la LAN de Cali hacia el servidor

16. CONFIGURACIÓN DE LISTAS DE CONTROL DE ACCESO

Realizamos la configuración para habilitar telnet sobre cada uno de los routers Medellín, Bogota y Cali, para tener acceso a cualquier dispositivo en la red.

Para ello habilitamos el acceso telnet en las line de comando vty 0 4, con nivel de privilegio 15.

Router Medellín

```
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#privilege level 15
MEDELLIN(config-line)#login local
MEDELLIN(config-line)#transport input telnet
MEDELLIN(config-line)#exit
MEDELLIN(config)#access-list 105 permit tcp host 192.168.1.99 host 192.168.1.98
eq telnet
MEDELLIN(config)#access-list 105 permit tcp host 192.168.1.99 host 192.168.1.131
eq telnet
MEDELLIN(config)#do wr
Building configuration...
[OK]
MEDELLIN(config)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#
```

Router Bogota

```
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#privilege level 15
BOGOTA(config-line)#login local
BOGOTA(config-line)#transport input telnet
BOGOTA(config-line)#exit
BOGOTA(config)#access-list 106 permit tcp host 192.168.1.98 host 192.168.1.131
eq telnet
```

```
BOGOTA(config)#access-list 106 permit tcp host 192.168.1.130 host 192.168.1.131
eq telnet
BOGOTA(config)#do wr
Building configuration...
[OK]
BOGOTA(config)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#
```

Router Cali

```
CALI#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
CALI(config)#line vty 0 4
```

```
CALI(config-line)#privilege level 15
```

```
CALI(config-line)#login local
```

```
CALI(config-line)#transport input telnet
```

```
CALI(config-line)#do wr
```

```
CALI(config)#access-list 107 permit tcp host 192.168.1.131 host 192.168.1.99 eq
telnet
```

```
CALI(config)#access-list 107 permit tcp host 192.168.1.131 host 192.168.1.98 eq
telnet
```

17.CONFIGURACIÓN PARA QUE SOLO EL SERVIDOR TENGA ACCESO A CUALQUIER DISPOSITIVO DE LA RED

Configuramos una Lista de Control de Acceso Extendida que permita tráfico desde el servidor hacia los equipos y viceversa, para ello se configuro en el router de Bogota y de esta manera denegaremos tráfico del equipo WS1.

Router Bogota

```
BOGOTA#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
BOGOTA(config)#access-list 104 deny tcp host 192.168.1.2 host 192.168.1.66
```

```
BOGOTA(config)#access-list 104 deny tcp host 192.168.1.2 host 192.168.1.67
```

```
BOGOTA(config)#access-list 104 permit tcp host 192.168.1.3 host 192.168.1.66
```

```
BOGOTA(config)#access-list 104 permit tcp host 192.168.1.3 host 192.168.1.67
```

```
BOGOTA(config)#interface se0/0/0
```

```
BOGOTA(config-if)#ip access-group 104 out
```

```
BOGOTA(config-if)#interface se0/0/1
```

```
BOGOTA(config-if)#ip access-group 104 out
```

```
BOGOTA(config-if)#
```

```
BOGOTA(config-if)#do wr
```

```
Building configuration...
```

```
[OK]
```

```
BOGOTA(config-if)#end
```

```
BOGOTA#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

18. CONFIGURACIÓN DE LA LAN DE MEDELLIN Y CALI PARA DENEGAR TRÁFICO A CUALQUIER OTRO DISPOSITIVO EN CUALQUIER PARTE DE LA RED

Configuramos una Lista de Control de Acceso Extendida sobre el router de Medellín; configurando la IP de origen y destino para permitir acceso al servidor, y así mismo denegando tráfico de otros segmentos de red.

Router Medellín para LAN

```
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#access-list 101 permit tcp host 192.168.1.34 host 192.168.1.3
eq www
MEDELLIN(config)#access-list 101 permit tcp host 192.168.1.36 host 192.168.1.3
eq www
MEDELLIN(config)#access-list 101 permit icmp host 192.168.1.34 host 192.168.1.3
MEDELLIN(config)#access-list 101 permit icmp host 192.168.1.36 host 192.168.1.3
MEDELLIN(config)#access-list 101 deny tcp any any
MEDELLIN(config)#interface serial 0/0/0
MEDELLIN(config-if)#ip access-group 101 out
MEDELLIN(config-if)#do wr
Building configuration...
[OK]
MEDELLIN(config-if)#end
MEDELLIN#
```

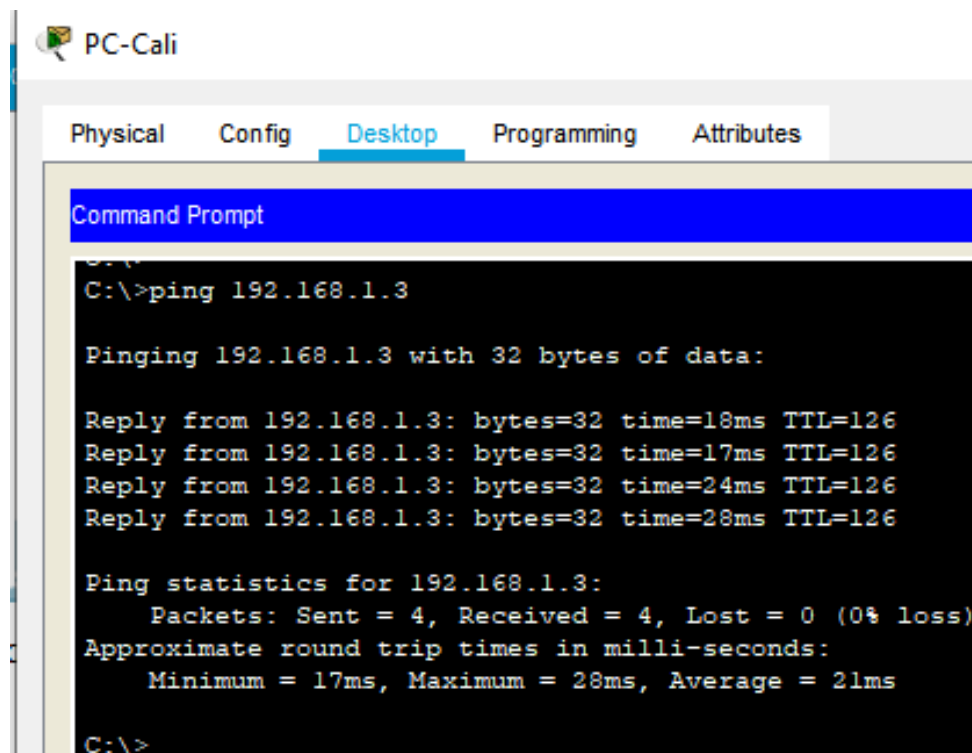
Router Cali para LAN

```
CALI# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#access-list 103 permit tcp host 192.168.1.66 host 192.168.1.3
CALI(config-if)#access-list 103 permit tcp host 192.168.1.67 host 192.168.1.3
CALI(config)#access-list 103 permit icmp host 192.168.1.66 host 192.168.1.3
CALI(config)#access-list 103 permit icmp host 192.168.1.67 host 192.168.1.3
CALI(config)#access-list 103 deny tcp any any
CALI(config)#interface serial0/0/0
CALI(config-if)#ip access-group 103 out
```

19.COMPROBAR LA RED INSTALADA

Probamos la configuración de listas de acceso para permitir y denegar tráfico desde la LAN de Medellín y Cali, de la misma manera se realizarán pruebas ICMP de acceso.

PING AL SERVIDOR DESDE LAN CALI



The screenshot shows a virtual desktop environment for a host named 'PC-Cali'. The 'Desktop' tab is selected in the top navigation bar. A 'Command Prompt' window is open, displaying the results of a ping command to the IP address 192.168.1.3. The output shows four successful replies with varying round-trip times and a summary of the ping statistics.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=18ms TTL=126
Reply from 192.168.1.3: bytes=32 time=17ms TTL=126
Reply from 192.168.1.3: bytes=32 time=24ms TTL=126
Reply from 192.168.1.3: bytes=32 time=28ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 28ms, Average = 21ms

C:\>
```

Figura 23. Prueba ICMP desde host de la LAN de Cali hacia el servidor

PING DESDE A PC-CALI A PC1_MEDELLÍN

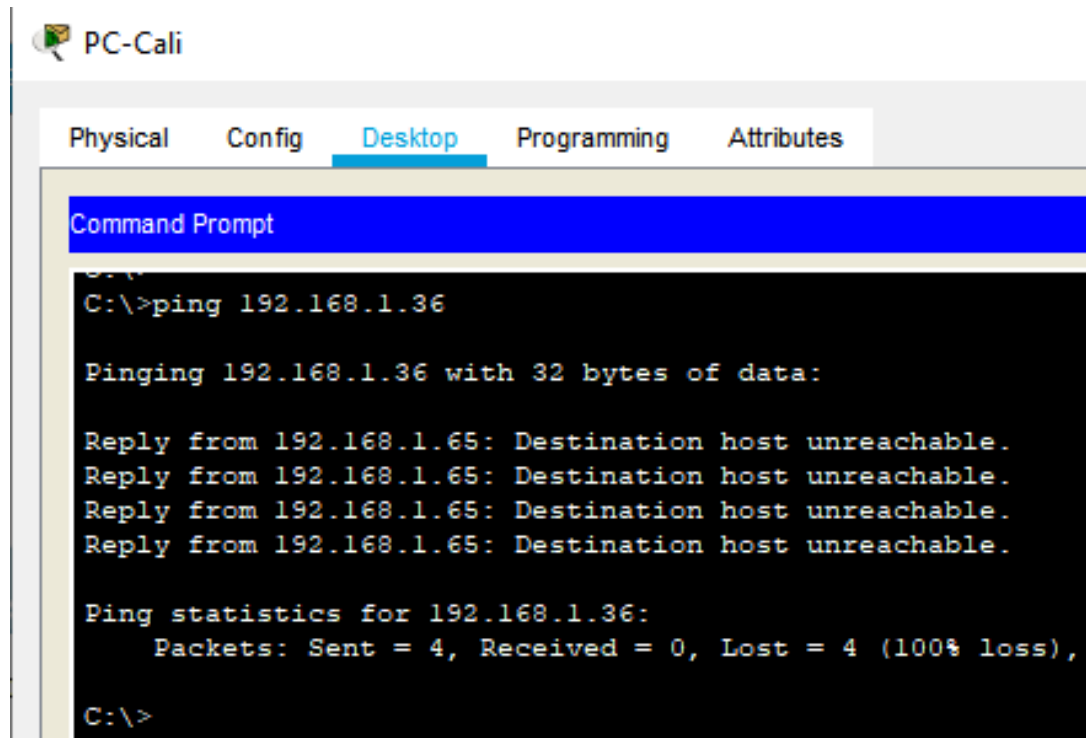


Figura 24. Prueba ICMP desde host de la LAN de Cali hacia el Medellín

PRUEBA DE ACCESO AL SERVIDOR DESDE LAN CALI



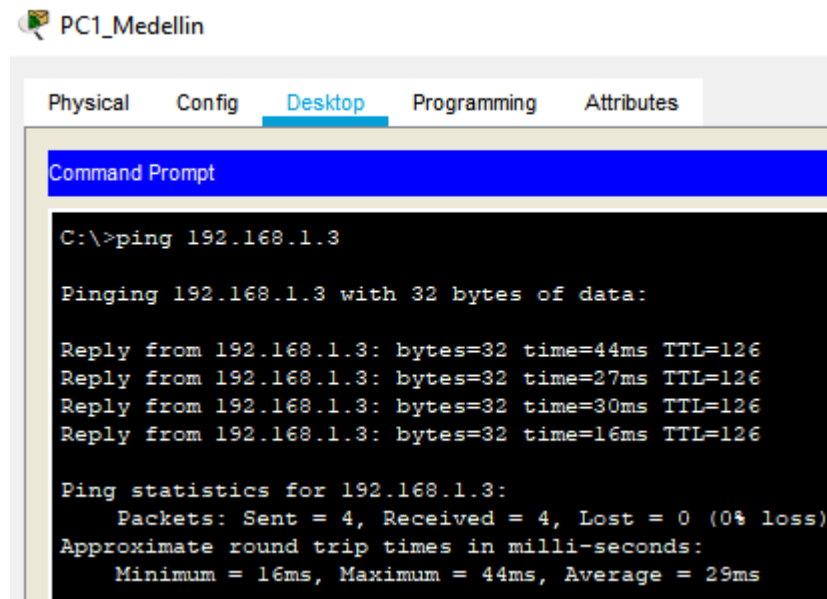
Figura 25. Acceso al servidor desde la LAN PC-Cali

PRUEBA DE ACCESO AL SERVIDOR DESDE LAN CALI



Figura 26. Acceso al servidor desde la LAN PC1-Cali

PING AL SERVIDOR DESDE LAN MEDELLIN



PC1_Medellin

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.1.3

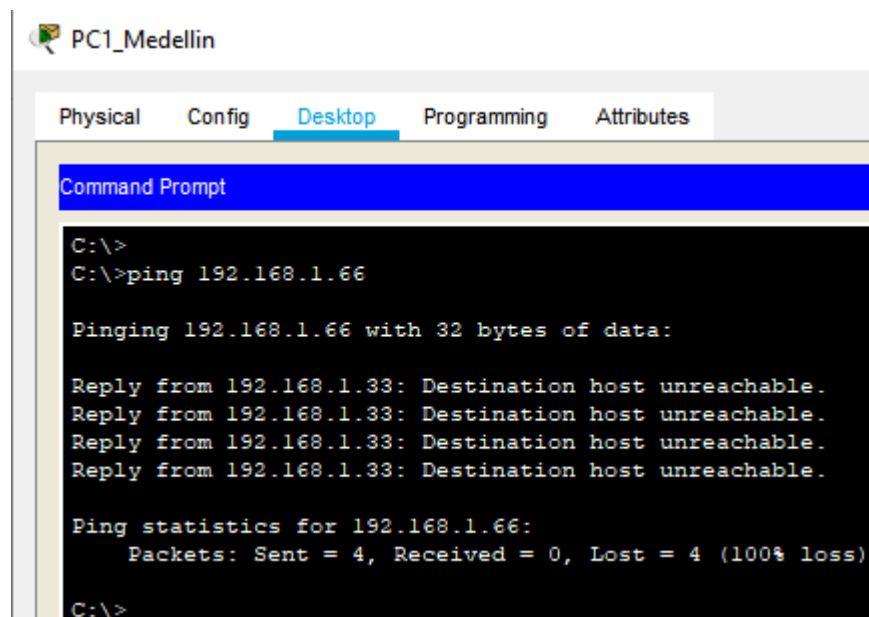
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=44ms TTL=126
Reply from 192.168.1.3: bytes=32 time=27ms TTL=126
Reply from 192.168.1.3: bytes=32 time=30ms TTL=126
Reply from 192.168.1.3: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 44ms, Average = 29ms
```

Figura 27. Prueba ICMP desde host de la LAN de Medellín hacia el servidor

PING DESDE PC1_MEDELLÍN A PC-CALI



PC1_Medellin

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

C:\>
```

Figura 28. Prueba ICMP desde host de la LAN de Medellín hacia Cali.

PRUEBA DE ACCESO AL SERVIDOR DESDE LAN MEDELLÍN



Figura 29. Acceso al servidor desde PC-Medellín

PRUEBA DE ACCESO AL SERVIDOR DESDE LAN MEDELLÍN

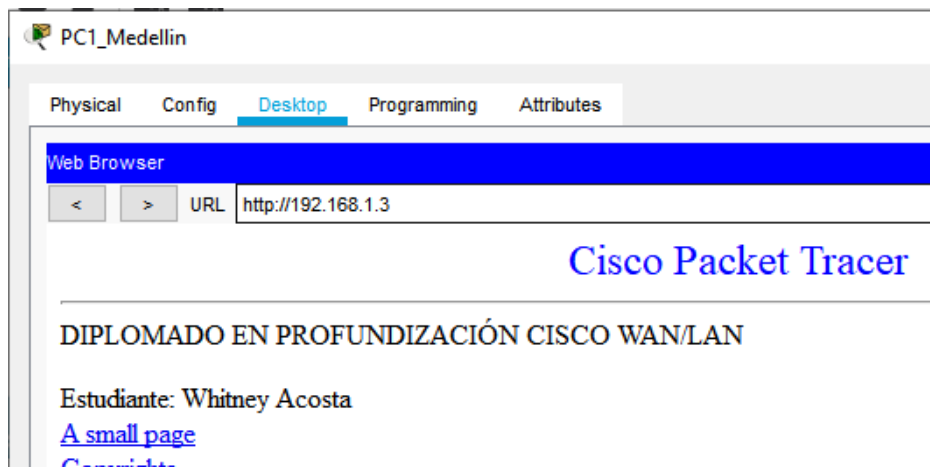


Figura 30. Acceso al servidor desde PC1_Medellín

**20.COMPLETAR LA SIGUIENTE TABLA DE CONDICIONES DE PRUEBA
PARA CONFIRMAR EL ÓPTIMO FUNCIONAMIENTO DE LA RED**

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Sin acceso
	WS_1	Router BOGOTA	Con acceso
	Servidor	Router CALI	Con acceso
	Servidor	Router MEDELLIN	Con acceso
TELNET	LAN del Router MEDELLIN	Router CALI	Sin acceso
	LAN del Router CALI	Router CALI	Con acceso
	LAN del Router MEDELLIN	Router MEDELLIN	Con acceso
	LAN del Router CALI	Router MEDELLIN	Sin acceso
PING	LAN del Router CALI	WS_1	Sin respuesta
	LAN del Router MEDELLIN	WS_1	Sin respuesta
	LAN del Router MEDELLIN	LAN del Router CALI	Sin respuesta
PING	LAN del Router CALI	Servidor	Con respuesta
	LAN del Router MEDELLIN	Servidor	Con respuesta
	Servidor	LAN del Router MEDELLIN	Con respuesta
	Servidor	LAN del Router CALI	Con respuesta
	Router CALI	LAN del Router MEDELLIN	Sin respuesta
	Router MEDELLIN	LAN del Router CALI	Sin respuesta

21. DESCRIPCIÓN DE ESCENARIO 2

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

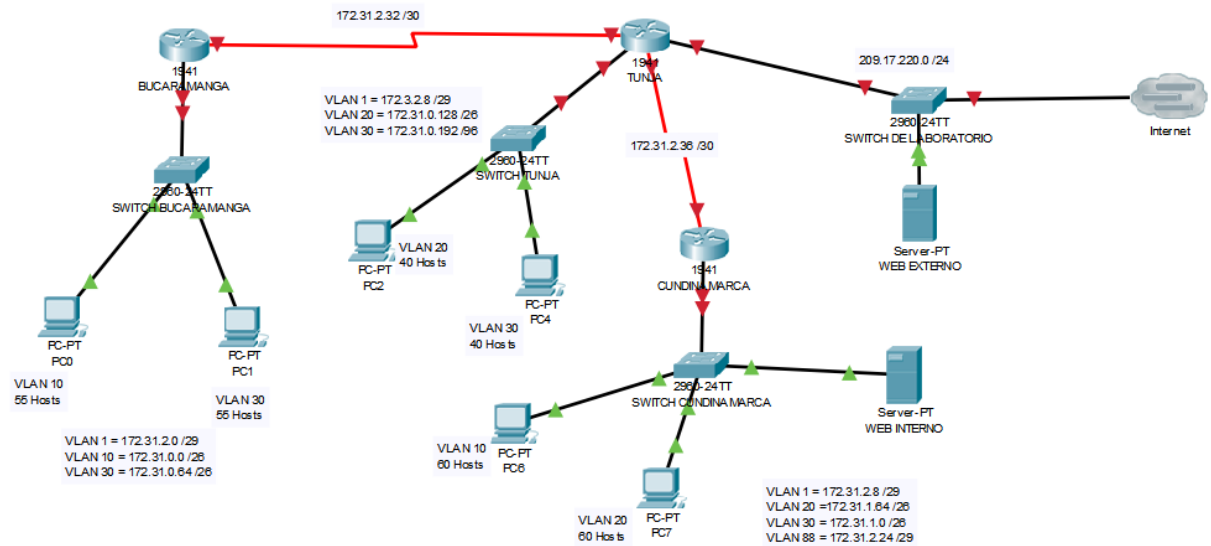


Figura 31. Escenario 2

22. CONFIGURACIÓN BÁSICA EN LOS ROUTER

Realizaremos la configuración básica en cada router, para ello procedo a dar inicio ingresando al router en modo configuración, y usando el comando hostname a continuación el nombre.

Router Bucaramanga

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#do wr
Building configuration...
[OK]
BUCARAMANGA(config)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

Switch Bucaramanga

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#do wr
Building configuration...
[OK]
BUCARAMANGA(config)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

Router Tunja

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname TUNJA

TUNJA(config)#do wr

Building configuration...

[OK]

TUNJA(config)#end

TUNJA#

%SYS-5-CONFIG_I: Configured from console by console

TUNJA#

Switch Tunja

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Switch_Tunja

Switch_Tunja(config)#do wr

Building configuration...

[OK]

Switch_Tunja(config)#end

Switch_Tunja#

%SYS-5-CONFIG_I: Configured from console by console

Router Cundinamarca

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname CUNDINAMARCA

CUNDINAMARCA(config)#do wr

Building configuration...

[OK]

CUNDINAMARCA(config)#end

CUNDINAMARCA#

%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#

Switch Cundinamarca

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Switch_Cundinamarca

Switch_Cundinamarca(config)#do wr

Building configuration...

[OK]

Switch_Cundinamarca(config)#end

Switch_Cundinamarca#

%SYS-5-CONFIG_I: Configured from console by console

Switch_Cundinamarca#

Switch del Laboratorio

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#hostname Switch_Laboratorio
```

```
Switch_Laboratorio(config)#do wr
```

Building configuration...

[OK]

```
Switch_Laboratorio(config)#end
```

```
Switch_Laboratorio#
```

%SYS-5-CONFIG_I: Configured from console by console

```
Switch_Laboratorio#
```

A continuación damos inicio a configurar contraseña enable sobre cada uno de los router

Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#enable password cisco
```

```
BUCARAMANGA(config)#service password-encryption
```

```
BUCARAMANGA(config)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config)#end
```

```
BUCARAMANGA#
```

%SYS-5-CONFIG_I: Configured from console by console

Router Tunja

```
TUNJA#configure terminal
```


Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#enable password cisco

TUNJA(config)#service password-encryption

TUNJA(config)#do wr

Building configuration...

[OK]

TUNJA(config)#end

TUNJA#

%SYS-5-CONFIG_I: Configured from console by console

Router Cundinamarca

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#enable password cisco

CUNDINAMARCA(config)#service password-encryption

CUNDINAMARCA(config)#do wr

Building configuration...

[OK]

CUNDINAMARCA(config)#end

CUNDINAMARCA#

%SYS-5-CONFIG_I: Configured from console by console

Continuamos con las configuraciones básicas en este espacio configuraremos la contraseña de consola para cada uno de los router

Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#line console 0
```

```
BUCARAMANGA(config-line)#password cisco
```

```
BUCARAMANGA(config-line)#login
```

```
BUCARAMANGA(config-line)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config-line)#end
```

```
BUCARAMANGA#
```

%SYS-5-CONFIG_I: Configured from console by console

Router Tunja

```
TUNJA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
TUNJA(config)#line console 0
```

```
TUNJA(config-line)#password cisco
```

```
TUNJA(config-line)#login
```

```
TUNJA(config-line)#do wr
```

Building configuration...

[OK]

```
TUNJA(config-line)#end
```

TUNJA#

Router Cundinamarca

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#line console 0

CUNDINAMARCA(config-line)#password cisco

CUNDINAMARCA(config-line)#login

CUNDINAMARCA(config-line)#do wr

Building configuration...

[OK]

CUNDINAMARCA(config-line)#end

CUNDINAMARCA#

%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#

Continuamos con la configuración de contraseñas para cada uno de los equipos sobre line vty.

Router Bucaramanga

BUCARAMANGA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

BUCARAMANGA(config)#line vty 0 4

BUCARAMANGA(config-line)#password cisco

BUCARAMANGA(config-line)#login

BUCARAMANGA(config-line)#end

BUCARAMANGA#

%SYS-5-CONFIG_I: Configured from console by console

Router Tunja

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#line vty 0 4

TUNJA(config-line)#password cisco

TUNJA(config-line)#login

TUNJA(config-line)#do wr

Building configuration...

[OK]

TUNJA(config-line)#end

TUNJA#

%SYS-5-CONFIG_I: Configured from console by console

Router Cundinamarca

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#line vty 0 4

CUNDINAMARCA(config-line)#password cisco

CUNDINAMARCA(config-line)#login

CUNDINAMARCA(config-line)#do wr

Building configuration...

[OK]

CUNDINAMARCA(config-line)#end

CUNDINAMARCA#

%SYS-5-CONFIG_I: Configured from console by console

A continuación realizaremos la configuración de banner para cada router con un corto mensaje indicando el acceso no autorizado a los equipos.

Router Bucaramanga

BUCARAMANGA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

BUCARAMANGA(config)#banner motd " !!!ACCESO SOLO A PERSONAS
AUTORIZADAS!!!

Enter TEXT message. End with the character "".

"

BUCARAMANGA(config)#do wr

Building configuration...

[OK]

BUCARAMANGA(config)#end

BUCARAMANGA#

%SYS-5-CONFIG_I: Configured from console by console

Router Tunja

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#banner motd " !!!ACCESO SOLO A PERSONAS
AUTORIZADAS!!!"

TUNJA(config)#do wr

Building configuration...

[OK]

TUNJA(config)#end

TUNJA#

%SYS-5-CONFIG_I: Configured from console by console

Router Cundinamarca

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#banner motd " !!!ACCESO SOLO A PERSONAS
AUTORIZADAS!!!"

CUNDINAMARCA(config)#do wr

Building configuration...

[OK]

CUNDINAMARCA(config)#end

CUNDINAMARCA#

%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#

23. CONFIGURACIÓN DE INTERFACES

En este espacio realizaremos la configuración de la interfaces WAN para esta primera configuración en el router de Bucaramanga, Tunja y Cundinamarca usaremos la serial 0/0/0 y serial 0/0/1.

Router Bucaramanga

BUCARAMANGA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

BUCARAMANGA(config)#interface serial0/0/0

BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252

BUCARAMANGA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Router Tunja

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252

TUNJA(config-if)#no shutdown

TUNJA(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

TUNJA(config-if)#interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

serial 0/0/1

TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252

```
TUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
TUNJA(config-if)#
TUNJA(config-if)#do wr
Building configuration...
[OK]
TUNJA(config-if)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#
```

```
Router Cundinamarca
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#interface serial 0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
CUNDINAMARCA(config-if)#do wr
Building configuration...
[OK]
CUNDINAMARCA(config-if)#end
CUNDINAMARCA#
```


23.1 CONFIGURACIÓN DE INTERFACES

En este espacio realizaremos las configuraciones pertinentes para cada sub-interfaz en los router de Bucaramanga y VLAN1 en el switch

Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#interface giga0/0
```

```
BUCARAMANGA(config-if)#no shutdown
```

```
BUCARAMANGA(config-if)#exit
```

```
BUCARAMANGA(config)#interface giga0/0.10
```

```
BUCARAMANGA(config-subif)#encapsulation dot1Q 10
```

```
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
```

```
BUCARAMANGA(config-subif)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config-subif)#exit
```

```
BUCARAMANGA(config)#interface giga0/0.20
```

```
BUCARAMANGA(config-subif)#
```

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

```
BUCARAMANGA(config-subif)#encapsulation dot1Q 20
```

```
BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
```

```
BUCARAMANGA(config-subif)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config-subif)#end
```

```
BUCARAMANGA#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
BUCARAMANGA#
```

Switch Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#interface vlan 1
```

```
BUCARAMANGA(config-if)#ip address 172.31.2.1 255.255.255.248
```

```
BUCARAMANGA(config-if)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config-if)#no shutdown
```

```
BUCARAMANGA(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
BUCARAMANGA(config-if)#end
```

```
BUCARAMANGA#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
BUCARAMANGA#
```

En este espacio realizaremos las configuraciones pertinentes para cada sub-interfaz en los router de Tunja y VLAN1 en el switch

Router Tunja

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#interface gi0/0

TUNJA(config-if)#no shutdown

TUNJA(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

TUNJA(config-if)#exit

TUNJA(config)#interface giga0/0.20

TUNJA(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

TUNJA(config-subif)#encapsulation dot1Q 20

TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192

TUNJA(config-subif)#do wr

Building configuration...

[OK]

TUNJA(config-subif)#exit

TUNJA(config)#interface giga0/0.30

TUNJA(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30,
changed state to up

TUNJA(config-subif)#encapsulation dot1Q 30

TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192

TUNJA(config)#interface gi0/1

TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0

TUNJA(config-if)#no shutdown

TUNJA(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

TUNJA(config-if)#do wr

Building configuration...

[OK]

TUNJA(config-if)#end

TUNJA#

TUNJA(config-subif)#do wr

Building configuration...

[OK]

TUNJA(config-subif)#end

TUNJA#

Switch Tunja

Switch_Tunja#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch_Tunja(config)#interface vlan 1

Switch_Tunja(config-if)#ip address 172.31.2.9 255.255.255.248

Switch_Tunja(config-if)#no shutdown

Switch_Tunja(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch_Tunja(config-if)#do wr

Building configuration...

[OK]

Switch_Tunja(config-if)#end

Switch_Tunja#

%SYS-5-CONFIG_I: Configured from console by console

Switch_Tunja#

En este espacio realizaremos las configuraciones pertinentes para cada sub-interfaz en los router de Cundinamarca y VLAN1 en el switch

Router Cundinamarca

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#interface giga0/0

CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#interface giga0/0.20

CUNDINAMARCA(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

CUNDINAMARCA(config-subif)#encapsulation dot1Q 20

CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192

CUNDINAMARCA(config)#interface giga0/0.30

CUNDINAMARCA(config-subif)#encapsulation dot1Q 30

CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192

CUNDINAMARCA(config-subif)#do wr

Building configuration...

[OK]

```
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#interface giga0/0.88
CUNDINAMARCA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.88, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.88,
changed state to up
CUNDINAMARCA(config-subif)#encapsulation dot1Q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#do wr
Building configuration...
[OK]
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
```

```
Switch Cundinamarca
Switch_Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Cundinamarca(config)#interface vlan 1
Switch_Cundinamarca(config-if)#ip address 172.31.2.9 255.255.255.248
Switch_Cundinamarca(config-if)#no shutdown
Switch_Cundinamarca(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch_Cundinamarca(config-if)#do wr
Building configuration...
```

23.2 ACTIVACIÓN DE VLANS EN SWITCH

En este espacio procedemos a habilitar y troncalizar las VLANs en los Switch de cada sede, de acuerdo a las configuraciones en los routers.

Switch Bucaramanga

VLAN 10 y 30

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#interface fa0/2
```

```
BUCARAMANGA(config-if)#switchport mode access
```

```
BUCARAMANGA(config-if)#switchport access vlan 10
```

```
BUCARAMANGA(config)#interface fas0/3
```

```
BUCARAMANGA(config-if)#switchport mode access
```

```
BUCARAMANGA(config-if)#switchport access vlan 30
```

```
BUCARAMANGA(config-if)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config-if)#exit
```

```
BUCARAMANGA(config)#interface fa0/1
```

```
BUCARAMANGA(config-if)#switchport mode trunk
```

```
BUCARAMANGA(config-if)#
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

BUCARAMANGA(config-if)#do wr

Building configuration...

[OK]

BUCARAMANGA(config-if)#end

BUCARAMANGA#

Switch Tunja

VLAN 20 Y 30

Switch_Tunja#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch_Tunja(config)#vlan 20

Switch_Tunja(config-vlan)#name 40_Hosts

Switch_Tunja(config-vlan)#exit

Switch_Tunja(config)#vlan 30

Switch_Tunja(config-vlan)#name 40-Hosts

Switch_Tunja(config-vlan)#exit

Switch_Tunja(config)#interface fa0/3

Switch_Tunja(config-if)#switchport mode access

Switch_Tunja(config-if)#switchport access vlan 30

Switch_Tunja(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

Switch_Tunja(config)#interface fa0/1

```
Switch_Tunja(config-if)#switchport mode trunk
Switch_Tunja(config-if)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch_Tunja(config-if)#do wr
Building configuration...
[OK]
Switch_Tunja(config-if)#end
```

```
Switch_Cundinamarca
VLAN 20 Y 30
Switch_Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Cundinamarca(config)#vlan 20
Switch_Cundinamarca(config-vlan)#name 60_Hosts
Switch_Cundinamarca(config-vlan)#exit
Switch_Cundinamarca(config)#interface fa0/3
Switch_Cundinamarca(config-if)#switchport mode access
Switch_Cundinamarca(config-if)#switchport access vlan 20
Switch_Cundinamarca(config-if)#exit
Switch_Cundinamarca(config)#vlan 30
Switch_Cundinamarca(config-vlan)#name 60-Hosts
Switch_Cundinamarca(config-vlan)#exit
Switch_Cundinamarca(config)#interface fa0/2
```

```
Switch_Cundinamarca(config-if)#switchport mode access
Switch_Cundinamarca(config-if)#switchport access vlan 30
Switch_Cundinamarca(config-if)#exit
Switch_Cundinamarca(config)#vlan 88
Switch_Cundinamarca(config-vlan)#name Web_Interno
Switch_Cundinamarca(config-vlan)#exit
Switch_Cundinamarca(config)#interface fa0/4
Switch_Cundinamarca(config-if)#switchport mode access
Switch_Cundinamarca(config-if)#switchport access vlan 88
Switch_Cundinamarca(config-if)#exit
Switch_Cundinamarca(config)#interface fa0/1
Switch_Cundinamarca(config-if)#switchport mode trunk
Switch_Cundinamarca(config-if)#
```

23.3 CONFIGURACIÓN DESCRIPCIÓN DE LAS INTERFACES

En este espacio se configuraran las descripciones de las interfaces sobre cada router.

Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#Interface serial 0/0/0
```

```
BUCARAMANGA(config-if)#description WAN
```

```
BUCARAMANGA(config-if)#EXIT
```

```
BUCARAMANGA(config)#interface Giga0/0
```

```
BUCARAMANGA(config-if)#description LAN_BUCARAMANGA
```

```
BUCARAMANGA(config-if)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config-if)#end
```

```
BUCARAMANGA#
```

%SYS-5-CONFIG_I: Configured from console by console

```
BUCARAMANGA#
```

Router Tunja

```
TUNJA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
TUNJA(config)#interface serial 0/0/0
```

```
TUNJA(config-if)#description WAN
```

```
TUNJA(config-if)#exit
```

```
TUNJA(config)#interface serial 0/0/1
TUNJA(config-if)#description LAN_TUNJA
TUNJA(config-if)#do wr
Building configuration...
[OK]
TUNJA(config-if)#end
TUNJA#
```

Router Cundinamarca

```
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface serial 0/0/0
TUNJA(config-if)#description WAN
TUNJA(config-if)#exit
TUNJA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface serial 0/0/1
TUNJA(config-if)#description WAN TUNJA-CUNDINAMARCA
TUNJA(config-if)#do wr
Building configuration...
[OK]
TUNJA(config-if)#exit
TUNJA(config)#interface giga0/0
TUNJA(config-if)#description LAN_TUNJA
TUNJA(config-if)#do wr
Router Cundinamarca
```

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#interface serial 0/0/0

CUNDINAMARCA(config-if)#description WAN_CUNDINAMARCA

CUNDINAMARCA(config-if)#interface giga0/0

CUNDINAMARCA(config-if)#description LAN_CUNDINAMARCA

CUNDINAMARCA(config-if)#do wr

Building configuration...

[OK]

CUNDINAMARCA(config-if)#end

CUNDINAMARCA#

24.ENRUTAMIENTO OSPF CON AUTENTICACIÓN

Realizamos enrutamiento bajo el protocolo OSFP con autenticación md5, el cual permite la autenticación de cada una de las rutas teniendo en cuenta la llave secreta sobre cada router.

Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#interface serial 0/0/0
```

```
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco-123
```

```
BUCARAMANGA(config-if)#ip ospf authentication message-digest
```

```
BUCARAMANGA(config)#interface giga0/0
```

```
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco-123
```

```
BUCARAMANGA(config-if)#ip ospf authentication message-digest
```

```
BUCARAMANGA(config-if)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config-if)#end
```

```

BUCARAMANGA#show ip ospf interface serial 0/0/0

Serial0/0/0 is up, line protocol is up
 Internet address is 172.31.2.33/30, Area 1
  Process ID 1, Router ID 172.31.2.33, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:01
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 209.17.220.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
BUCARAMANGA#

```

Figura 32. Configuración OSPF con autenticación para Bucaramanga

Router Tunja

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco-123

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#

TUNJA(config)#interface serial 0/0/1

TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco-123

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#exit

TUNJA(config)#interface giga0/0

TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco-123

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#exit

TUNJA(config)#interface giga0/1

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco-123

TUNJA(config-if)#

10:02:34: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
10:02:34: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
TUNJA(config-if)#do wr
Building configuration...

```
TUNJA#show ip ospf interface serial 0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.2.34/30, Area 1
  Process ID 1, Router ID 209.17.220.1, Network Type POI
  Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priorit
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40
  5
    Hello due in 00:00:07
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 172.31.2.33
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
TUNJA#
```

Figura 33. Configuración OSPF con autenticación para Tunja

Router Cundinamarca

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#interface serial 0/0/0

CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco-123

CUNDINAMARCA(config-if)#ip ospf authentication message-digest

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#interface giga0/0

CUNDINAMARCA(config-if)#

10:06:04: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.1 on Serial0/0/0 from
LOADING to FULL, Loading Done

ip ospf authentication message-digest

CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco-123

CUNDINAMARCA(config-if)#do wr

Building configuration..

```
CUNDINAMARCA#sho ip ospf interface serial 0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.2.38/30, Area 1
  Process ID 1, Router ID 172.31.2.38, Network Type
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Pri
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wai
5
  Hello due in 00:00:02|
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 209.17.220.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
CUNDINAMARCA#
```

Figura 34. Configuración OSPF con autenticación para Cundinamarca

25. AUTENTICACIÓN LOCAL CON AAA

Se realizó la configuración de autenticación local AAA para los routers de la topología actual, para ello usaremos el comando `aaa new-model` el cual permite configuraciones a nivel de seguridad local y remota.

Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#aaa new-model
```

```
BUCARAMANGA(config)#aaa authentication login default local
```

```
BUCARAMANGA(config)#line console 0
```

```
BUCARAMANGA(config-line)#login authentication default
```

```
BUCARAMANGA(config-line)#exit
```

```
BUCARAMANGA(config)#exit
```

```
BUCARAMANGA(config)#ip domain-name whitney.com
```

```
BUCARAMANGA(config)#crypto key generate rsa
```

% You already have RSA keys defined named BUCARAMANGA.whitney.org .

% Do you really want to replace them? [yes/no]: yes

The name for the keys will be: BUCARAMANGA.whitney.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
BUCARAMANGA(config)#aaa authentication login LOCAL_LOGIN local
```

*mar. 1 9:4:55.955: %SSH-5-ENABLED: SSH 2 has been enabled

```
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#transport input ssh
BUCARAMANGA(config-line)#login authentication LOCAL_LOGIN
BUCARAMANGA(config-line)#
BUCARAMANGA(config-line)#
BUCARAMANGA(config-line)#do wr
Building configuration...
[OK]
BUCARAMANGA(config-line)#end
BUCARAMANGA#
*mar. 01, 09:11:33.1111: SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

Router Tunja

```
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login default local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication default
TUNJA(config-line)#exit
TUNJA(config)#ip domain-name whitney.com
TUNJA(config)#crypto key generate rsa
The name for the keys will be: TUNJA.whitney.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
```

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

TUNJA(config)#aaa authentication login LOCAL_LOGIN local

*mar. 1 0:28:13.245: %SSH-5-ENABLED: SSH 1.99 has been enabled

TUNJA(config)#line vty 0 4

TUNJA(config-line)#transport input ssh

TUNJA(config-line)#login authentication LOCAL_LOGIN

TUNJA(config-line)#

TUNJA(config-line)#do wr

Building configuration...

[OK]

TUNJA(config-line)#end

TUNJA#

Router Cundinamarca

CUNDINAMARCA #configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#aaa new-model

CUNDINAMARCA(config)#aaa authentication login default local

CUNDINAMARCA(config)#line console 0

CUNDINAMARCA(config-line)#login authentication default

CUNDINAMARCA(config-line)#exit

CUNDINAMARCA(config)#ip domain-name whitney.com

CUNDINAMARCA(config)#crypto key generate rsa

% You already have RSA keys defined named CUNDINAMARCA.whitney.com .

% Do you really want to replace them? [yes/no]: yes

The name for the keys will be: CUNDINAMARCA.whitney.com

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

CUNDINAMARCA(config)#aaa authentication LOCAL_LOGIN local

*mar. 1 0:43:36.828: %SSH-5-ENABLED: SSH 1.99 has been enabled

CUNDINAMARCA(config)#aaa authentication login LOCAL_LOGIN local

CUNDINAMARCA(config)#line vty 0 4

CUNDINAMARCA(config-line)#transport input ssh

CUNDINAMARCA(config-line)#login authentication LOCAL_LOGIN

CUNDINAMARCA(config-line)#

CUNDINAMARCA(config-line)#do wr

Building configuration...

[OK]

CUNDINAMARCA(config-line)#end

CUNDINAMARCA#

%SYS-5-CONFIG_I: Configured from console by console

26. MAXIMO DE INTENTOS PARA ACCEDER AL ROUTER Y TIEMPO DE INGRESO

Realizamos configuración sobre cada router el máximo de intentos de ingreso al router, determinado en 3 intentos y en tiempo de ingreso al router en 60 segundos.

Router Bucaramanga

BUCARAMANGA#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

BUCARAMANGA(config)#ip ssh time-out 60

BUCARAMANGA(config)#ip ssh authentication-retries 3

BUCARAMANGA(config)#do wr

Building configuration...

[OK]

BUCARAMANGA(config)#end

BUCARAMANGA#

*mar. 01, 02:52:35.5252: SYS-5-CONFIG_I: Configured from console by console

Router Tunja

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#ip ssh time-out 60

TUNJA(config)#ip ssh authentication-retries 3

TUNJA(config)#do wr

Building configuration...

[OK]

TUNJA(config)#end

```
TUNJA#
Router Cundinamarca
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip ssh time-out 60
CUNDINAMARCA(config)#ip ssh authentication-retries 3
CUNDINAMARCA(config)#do wr
Building configuration...
[OK]
CUNDINAMARCA(config)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```


27. CONFIGURACIÓN DE SERVIDOR TFTP PARA ALMACENAMIENTO DE ARCHIVOS EN LOS ROUTER

En este espacio crearemos un servidor TFTP para lograr almacenamiento, iniciaremos con el router de Cundinamarca

Router Cundinamarca

```
CUNDINAMARCA#copy run tftp
```

```
Address or name of remote host []? 172.31.2.227
```

```
Destination filename [CUNDINAMARCA-config]?
```

```
Writing running-config...!!
```

```
[OK - 2044 bytes]
```

```
2044 bytes copied in 0.011 secs (185818 bytes/sec)
```

```
CUNDINAMARCA#
```

Router Tunja

```
TUNJA#copy run tftp
```

```
Address or name of remote host []? 209.17.220.2
```

```
Destination filename [TUNJA-config]?
```

```
Writing running-config....!!
```

```
[OK - 1771 bytes]
```

```
1771 bytes copied in 3.015 secs (587 bytes/sec)
```

```
TUNJA#
```

Router Bucaramanga

BUCARAMANGA#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

BUCARAMANGA#copy run tftp

Address or name of remote host []? 172.31.2.227

Destination filename [BUCARAMANGA-config]?

Writing running-config....!!

[OK - 1968 bytes]

1968 bytes copied in 3.077 secs (639 bytes/sec)

BUCARAMANGA#

28. CONFIGURACIÓN DE DHCP PARA BUCARAMANGA Y CUNDINAMARCA CON IP HELPER-ADDRESS DESDE TUNJA

En este espacio se realizara configuración de DHCP para las sedes de Bucaramanga y Cundinamarca con ip helper-address sobre cada router seleccionando la interfaz del router de Tunja, el cual se encargaría de realizar la entrega de direccionamiento IP.

Para ello ingresamos al router de Tunja, y allí mismo realizaremos la exclusión de direccionamiento IP de cada segmento de red para la sede de Cundinamarca.

Router Tunja – DHCP Cundinamarca

```
TUNJA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.94
```

```
TUNJA(config)#ip dhcp pool VLAN_20
```

```
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
```

```
TUNJA(dhcp-config)#default-router 172.31.1.65
```

```
TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.30
```

```
TUNJA(config)#ip dhcp pool VLAN_30
```

```
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
```

```
TUNJA(dhcp-config)#default-router 172.31.1.1
```

```
TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp pool VLAN_20
```

```
TUNJA(dhcp-config)#no network 172.31.1.34 255.255.255.192
```

```
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
```

```
TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp exc
TUNJA(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.30
TUNJA(config)#ip dhcp pool VLAN_88
TUNJA(dhcp-config)#network 172.31.2.24 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.25
TUNJA(dhcp-config)#do wr
TUNJA(dhcp-config)#end
TUNJA#
```

Router Cundinamarca

```
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#interface giga0/0.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#interface giga0/0.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

A continuación se evidencia que los equipos de la red de Cundinamarca ya se encuentran recibiendo dirección IP por DHCP de acuerdo a la configuración en el router de Tunja.

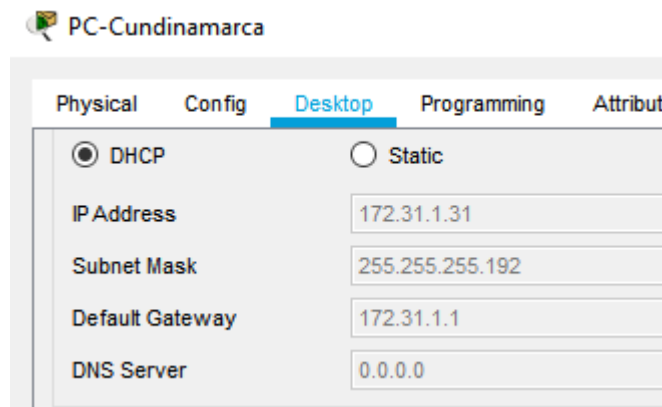


Figura 35. Direcccionamiento IP por DHCP desde el router de Tunja

Continuamos con la configuración de direccionamiento DHCP para el router de Bucaramanga para ello ingresamos al router de Tunja, y allí mismo realizaremos la exclusión de direccionamiento IP de cada segmento de red para la sede de Cundinamarca.

Router Tunja – DHCP Bucaramanga

```
TUNJA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
TUNJA(config)#
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.30
```

```
TUNJA(config)#ip dhcp pool VLAN_10
```

```
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
```

```
TUNJA(dhcp-config)#default-router 172.31.0.1
```

```
TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.94
TUNJA(config)#ip dhcp pool VLAN-30
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65
TUNJA(dhcp-config)#exit
TUNJA(config)#do wr
Building configuration...
[OK]
TUNJA(config)#end
TUNJA#
```

```
Router Bucaramanga
BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface giga0/0.10
BUCARAMANGA(config-subif)#ip helper
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#interface giga0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#do wr
Building configuration...
[OK]
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
```

A continuación se evidencia que los equipos de la red de Bucaramanga ya se encuentran recibiendo dirección IP por DHCP de acuerdo a la configuración en el router de Tunja.

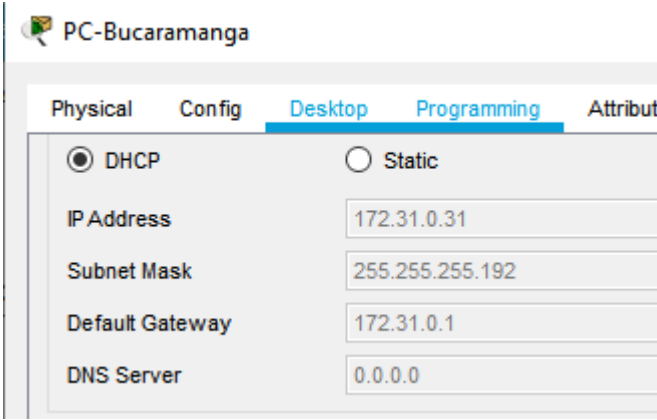


Figura 36. Direccionamiento IP por DHCP desde el router de Bucaramanga

29. HABILITAR OPCIONES EN PUERTO DE CONSOLA Y TERMINAL VIRTUAL

En este espacio se realizara la configuración adecuada para puerto de consola en el router y así mismo un tiempo permitido de ingreso de 0 a 60 segundos.

Router Bucaramanga

```
BUCARAMANGA(config)#enable password cisco
```

```
BUCARAMANGA(config)#service password-encryption
```

```
BUCARAMANGA(config)#line vty 0 4
```

```
BUCARAMANGA(config-line)#password cisco
```

```
BUCARAMANGA(config-line)#exec-t
```

```
BUCARAMANGA(config-line)#exec-timeout 0 60
```

```
BUCARAMANGA(config-line)#login
```

```
BUCARAMANGA(config-line)#logging synchronous
```

```
BUCARAMANGA(config-line)#exit
```

```
BUCARAMANGA(config)#service password-encryption
```

```
BUCARAMANGA(config)#
```

```
BUCARAMANGA(config)#do wr
```

Building configuration...

[OK]

```
BUCARAMANGA(config)#end
```

```
BUCARAMANGA#
```

```
BUCARAMANGA(config)#username whitney password cisco
```

```
BUCARAMANGA(config)#line console 0
```

```
BUCARAMANGA(config-line)#login local
```

```
BUCARAMANGA(config-line)#password cisco
```



```
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#
BUCARAMANGA(config)#do wr
Building configuration...
[OK]
BUCARAMANGA(config)#end
BUCARAMANGA#
```

Router Tunja

```
TUNJA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#username whitney password cisco
TUNJA(config)#line console 0
TUNJA(config-line)#login local
TUNJA(config-line)#password cisco
TUNJA(config-line)#exit
TUNJA(config)#service password-encryption
TUNJA(config)#enable password cisco
TUNJA(config)#service password-encryption
TUNJA(config)#line vty 0 4
TUNJA(config-line)#password cisco
TUNJA(config-line)#exec-timeout 0 60
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#exit
```

TUNJA(config)#service password-encryption

TUNJA(config)#

TUNJA(config)#do wr

Building configuration...

[OK]

TUNJA(config)#end

TUNJA#

Router Cundinamarca

CUNDINAMARCA#configure termina

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#username whitney password cisco

CUNDINAMARCA(config)#line console 0

CUNDINAMARCA(config-line)#login local

CUNDINAMARCA(config-line)#password cisco

CUNDINAMARCA(config-line)#exit

CUNDINAMARCA(config)#service password-encryption

CUNDINAMARCA(config)#line vty 0 4

CUNDINAMARCA(config-line)#password cisco

CUNDINAMARCA(config-line)#exec-timeout 0 60

CUNDINAMARCA(config-line)#login

CUNDINAMARCA(config-line)#loggin synchronous

CUNDINAMARCA(config-line)#exit

CUNDINAMARCA(config)#service password-encryption

CUNDINAMARCA(config)#do wr

30.CONFIGURACIÓN DE NAT ESTATICO PARA EL WEB SERVER Y SOBRECARGA PAT

Se realiza configuración de NAT estático para web servers, anunciando la interfaces inside como serial 0/0/1 y outside como serial 0/0/0, gi0/0, para el servidor interno.

Router Tunja – Server Web Interno

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#ip nat inside source static 172.31.2.227 209.17.220.0

TUNJA(config)#interface serial 0/0/1

TUNJA(config-if)#ip nat inside

TUNJA (config-if)#interface serial 0/0/0

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#interface giga0/0

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#

TUNJA(config-if)#do wr

Building configuration...

[OK]

TUNJA(config-if)#end

TUNJA#

```
TUNJA#sh ip nat translations
Pro  Inside global      Inside local          Outside local          Outside global
icmp 209.17.220.0:16   172.31.2.227:16      172.31.0.31:16        172.31.0.31:16
icmp 209.17.220.0:17   172.31.2.227:17      172.31.0.31:17        172.31.0.31:17
icmp 209.17.220.0:18   172.31.2.227:18      172.31.0.31:18        172.31.0.31:18
icmp 209.17.220.0:19   172.31.2.227:19      172.31.0.31:19        172.31.0.31:19
```

Figura 37. Configuración NAT estático para Web Server Interno

Router Tunja – Server Web Externo

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#ip nat inside source static 209.17.220.2 200.200.200.7

TUNJA(config)#interface giga0/1

TUNJA(config-if)#ip nat inside

TUNJA(config-if)#interface serial 0/0/0

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#interface giga0/0

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#

```
TUNJA#sh ip nat translations
Pro  Inside global      Inside local          Outside local          Outside global
icmp 200.200.200.7:5   209.17.220.2:5       172.31.0.95:5         172.31.0.95:5
icmp 200.200.200.7:6   209.17.220.2:6       172.31.0.95:6         172.31.0.95:6
icmp 200.200.200.7:7   209.17.220.2:7       172.31.0.95:7         172.31.0.95:7
icmp 200.200.200.7:8   209.17.220.2:8       172.31.0.95:8         172.31.0.95:8
```

Figura 38. Configuración NAT estático para Web Server Externo

31. SOBRECARGA PAT PARA LOS DEMÁS EQUIPOS

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA (config)#ip nat inside source static tcp 209.17.220.2 80 200.200.200.7 80

TUNJA (config)#ip nat inside source static tcp 209.17.220.2 80 200.200.200.7 80

TUNJA (config)#do wr

Building configuration...

[OK]

TUNJA(config)#end

TUNJA#



Figura 39. Configuración PAT de sobrecarga

32. ESTABLECER ACL PARA EL ESCENARIO 2

32.1 Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

Se realiza configuración de lista de acceso extendida 101, pen el router de Cundinamarca para permitir tráfico de los host con red 172.31.1.64/26 (VLAN20), hacia la red interna de Tunja 172.31.0.129 /26 y 172.31.0.193 /26.

Adicionalmente se crea una lista de acceso 110 para denegar tráfico hacia cualquier host. A través de comandos any any.

Router Cundinamarca – VLAN 20

CUNDINAMARCA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
CUNDINAMARCA(config)#access-list 110 permit ip 172.31.1.64 0.0.0.63
172.31.0.129 0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 110 permit ip 172.31.1.64 0.0.0.63
172.31.0.193 0.0.0.63
```

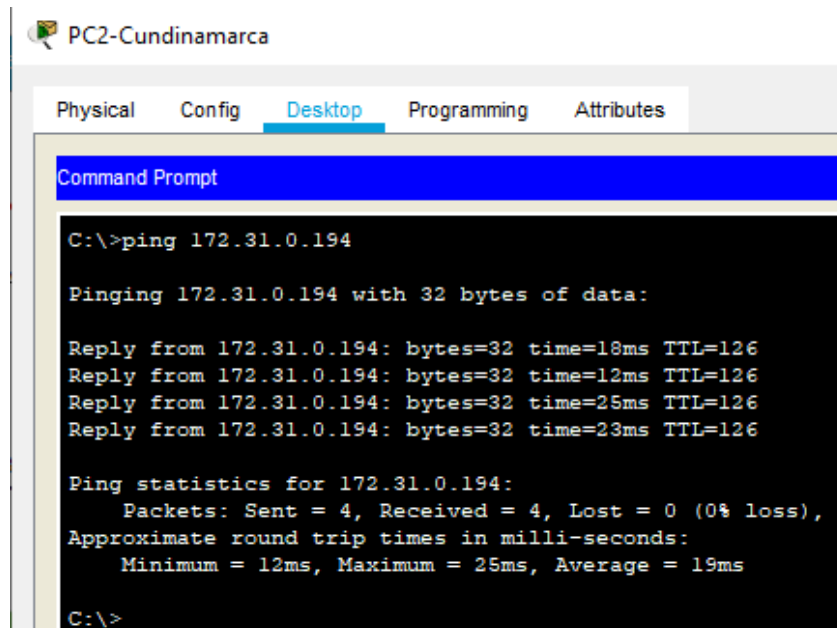
```
CUNDINAMARCA(config)#access-list 110 deny ip any any
```

```
CUNDINAMARCA(config)#interface serial 0/0/0
```

```
CUNDINAMARCA(config-if)#ip access-group 110 out
```

```
CUNDINAMARCA(config-if)#do wr
```

Building configuration...



```
PC2-Cundinamarca
Physical  Config  Desktop  Programming  Attributes

Command Prompt

C:\>ping 172.31.0.194

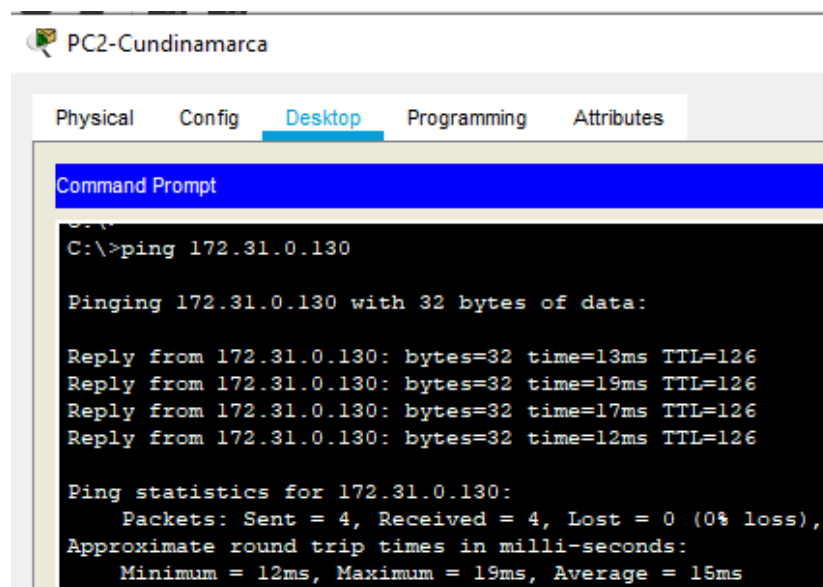
Pinging 172.31.0.194 with 32 bytes of data:

Reply from 172.31.0.194: bytes=32 time=18ms TTL=126
Reply from 172.31.0.194: bytes=32 time=12ms TTL=126
Reply from 172.31.0.194: bytes=32 time=25ms TTL=126
Reply from 172.31.0.194: bytes=32 time=23ms TTL=126

Ping statistics for 172.31.0.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 25ms, Average = 19ms

C:\>
```

Figura 40. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja.



```
PC2-Cundinamarca
Physical  Config  Desktop  Programming  Attributes

Command Prompt

C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.0.130: bytes=32 time=13ms TTL=126
Reply from 172.31.0.130: bytes=32 time=19ms TTL=126
Reply from 172.31.0.130: bytes=32 time=17ms TTL=126
Reply from 172.31.0.130: bytes=32 time=12ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 19ms, Average = 15ms
```

Figura 41. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja

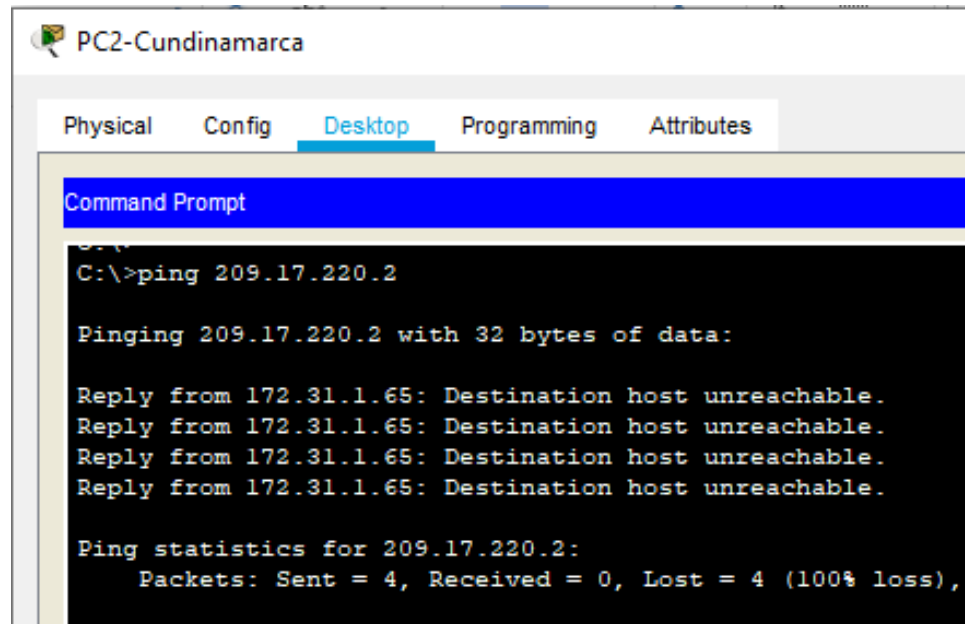


Figura 42. Ping desde PC Cundinamarca hacia Internet.

32.2 Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

Se realiza configuración de lista de acceso extendida 120, en el router de Tunja para permitir tráfico de los host con red 172.31.0.128 /26 (VLAN20), hacia la red interna de Cundinamarca 172.31.1.64 /26 (VLAN20) y a la (VLAN10) en Bucaramanga 172.31.0.0 /26

Adicionalmente se crea una lista de acceso 120 para denegar tráfico hacia cualquier host. A través de comandos any any.

Router Tunja VLAN 20 – VLAN 20 Cundinamarca y VLAN 10 de Bucaramanga

```
TUNJA# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
TUNJA(config)#access-list 120 permit ip 172.31.0.128 0.0.0.30 172.31.1.64 0.0.0.63
```

```
TUNJA(config)#access-list 120 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
```

```
TUNJA(config)#access-list 120 deny ip any
```

```
TUNJA(config)#interface serial 0/0/1
```

```
TUNJA(config-if)#ip access-group 120 out
```

```
TUNJA(config-if)#interface serial 0/0/0
```

```
TUNJA(config-if)#ip access-group 120 out
```

```
TUNJA(config-if)#
```

```
TUNJA(config-if)#
```

```
TUNJA(config-if)#do wr
```

PC2-TUNJA

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=15ms TTL=126
Reply from 172.31.1.66: bytes=32 time=14ms TTL=126
Reply from 172.31.1.66: bytes=32 time=14ms TTL=126
Reply from 172.31.1.66: bytes=32 time=13ms TTL=126

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 15ms, Average = 14ms

C:\>
```

Figura 43. Ping desde PC Tunja VLAN 20 a PC Cundinamarca VLAN 20

PC2-TUNJA

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 172.31.0.31

Pinging 172.31.0.31 with 32 bytes of data:

Reply from 172.31.0.31: bytes=32 time=19ms TTL=126
Reply from 172.31.0.31: bytes=32 time=14ms TTL=126
Reply from 172.31.0.31: bytes=32 time=10ms TTL=126
Reply from 172.31.0.31: bytes=32 time=14ms TTL=126

Ping statistics for 172.31.0.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 19ms, Average = 14ms

C:\>
```

Figura 44. Ping desde PC Tunja VLAN 20 a PC Bucaramanga VLAN 10

32.3 Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10

Se realiza configuración de lista de acceso extendida 101, en el router de Bucaramanga sobre la (VLAN30) con red 172.31.0.64 /26 para permitir tráfico hacia Internet y a cualquier equipo de la (VLAN10) con red 172.31.0.0 /26

Router Bucaramanga VLAN 30 hacia Internet y VLAN 10

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

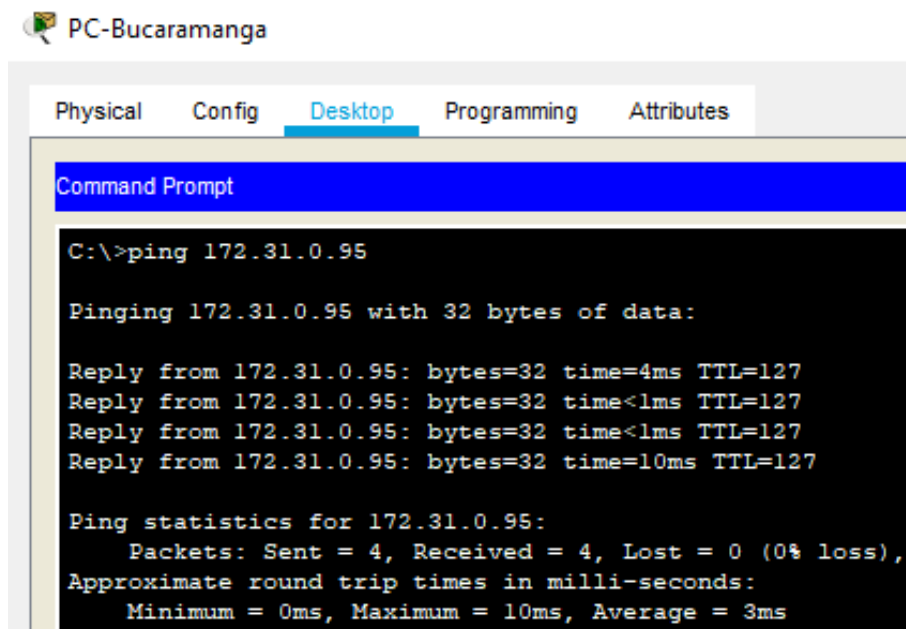
```
BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63 172.31.0.0  
0.0.0.63
```

```
BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63  
209.17.220.0 0.0.0.255
```

```
BUCARAMANGA(config)#interface giga0/0
```

```
BUCARAMANGA(config-if)#ip access-group 101 out
```

```
BUCARAMANGA(config-if)#
```



```
PC-Bucaramanga
Physical  Config  Desktop  Programming  Attributes

Command Prompt

C:\>ping 172.31.0.95

Pinging 172.31.0.95 with 32 bytes of data:

Reply from 172.31.0.95: bytes=32 time=4ms TTL=127
Reply from 172.31.0.95: bytes=32 time<1ms TTL=127
Reply from 172.31.0.95: bytes=32 time<1ms TTL=127
Reply from 172.31.0.95: bytes=32 time=10ms TTL=127

Ping statistics for 172.31.0.95:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

Figura 45. Ping desde PC Bucaramanga VLAN 30 hacia VLAN 10 PC Bucaramanga

32.4 Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

Se realiza configuración de lista de acceso extendida 103, en el router de Bucaramanga sobre la (VLAN10) con red 172.31.0.0 /26 para permitir tráfico hacia la (VLAN20) con red 172.31.1.64 /26 en Cundinamarca y (VLAN20) con red 172.31.0.128 /26 en Tunja

Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#access-list 103 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
```

```
BUCARAMANGA(config)#access-list 103 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
```

```
BUCARAMANGA(config)#access-list 103 deny ip 172.31.0.0 0.0.0.63 209.17.220.2 0.0.0.255
```

```
BUCARAMANGA(config)#
```

```
BUCARAMANGA(config)#interface serial 0/0/0
```

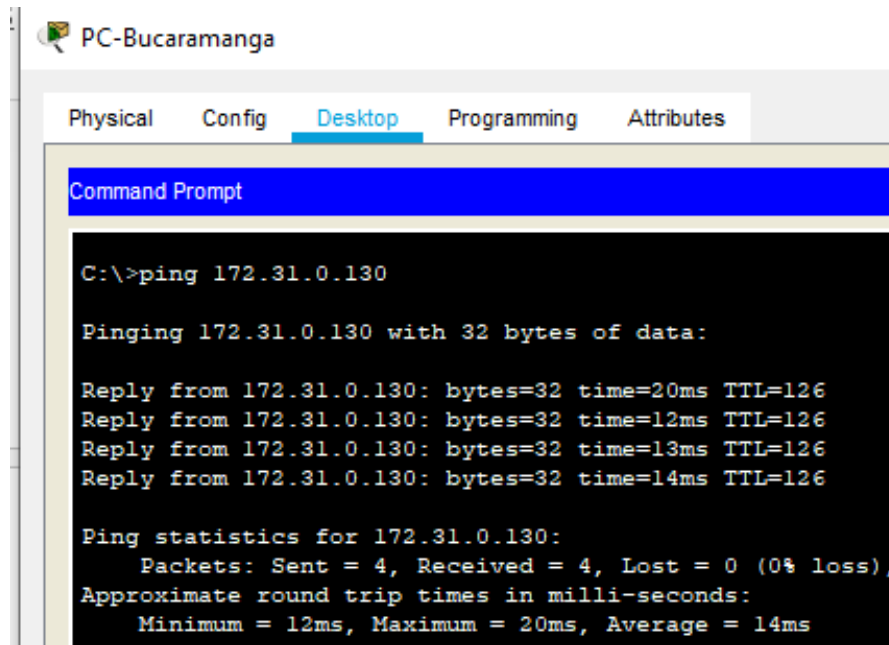
```
BUCARAMANGA(config-if)#ip access-group 103 out
```

```
BUCARAMANGA(config-if)#
```

```
BUCARAMANGA(config-if)#end
```

```
BUCARAMANGA#
```

```
*mar. 01, 04:33:25.3333: SYS-5-CONFIG_I: Configured from console by console
```



The screenshot shows a window titled "PC-Bucaramanga" with tabs for Physical, Config, Desktop (selected), Programming, and Attributes. A Command Prompt is open, displaying the following text:

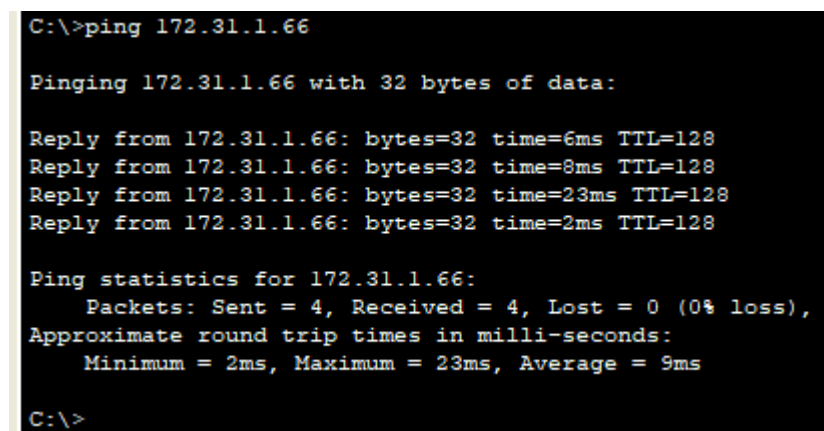
```
C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.0.130: bytes=32 time=20ms TTL=126
Reply from 172.31.0.130: bytes=32 time=12ms TTL=126
Reply from 172.31.0.130: bytes=32 time=13ms TTL=126
Reply from 172.31.0.130: bytes=32 time=14ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 20ms, Average = 14ms
```

Figura 46. Ping desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Tunja



The screenshot shows a Command Prompt window with the following text:

```
C:\>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=6ms TTL=128
Reply from 172.31.1.66: bytes=32 time=8ms TTL=128
Reply from 172.31.1.66: bytes=32 time=23ms TTL=128
Reply from 172.31.1.66: bytes=32 time=2ms TTL=128

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 23ms, Average = 9ms

C:\>
```

Figura 47. Ping desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Cundinamarca

32.5 Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

Se realiza configuración de lista de acceso extendida 120, en el router de Tunja sobre la (VLAN30) con red 172.31.0.128 /26 para permitir tráfico hacia Internet y servidor FTP de Internet.

Router Tunja

```
TUNJA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
TUNJA(config)#access-list 120 permit ip 172.31.0.192 0.0.0.63 172.31.2.224 0.0.0.63
```

```
TUNJA(config)#access-list 120 permit tcp 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255
```

```
TUNJA(config)#access-list 120 permit ip 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255
```

```
TUNJA(config)#access-list 120 permit tcp 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255
```

```
TUNJA(config)#do wr
```

32.6 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

Se realiza la configuración para VLAN1 desde Bucaramanga a Tunja y Cundinamarca

Bucaramanga

```
BUCARAMANGA#confi ter
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUCARAMANGA(config)#access-list 101 deny ip 172.31.2.0 0.0.0.63 172.31.2.8  
0.0.0.63
```

```
BUCARAMANGA(config)#interface fa0/1
```

```
BUCARAMANGA(config-if)#ip access-group 101 out
```

```
BUCARAMANGA(config-if)#do wr
```


33.CONCLUSIONES

Posteriormente, arribamos a la conclusión en el que hoy en día en el área de las telecomunicaciones nos es necesario escudriñar y comprender el uso y aplicaciones de conceptos de CCNA, a nivel personal y profesional, con el fin de desarrollar habilidades de destreza que nos permitan entender desde el uso de comandos como ping, nslookup, traceroute, entre otros. Hasta entender el funcionamiento de un enrutamiento avanzado usando OSPFv3 y EIGRP como distribución, permitiéndonos ahondar en nuestros conocimientos para tener las bases de apoyo para el futuro desarrollo de problemáticas que se presenten en un ambiente real y a su vez comprender la importancia de implementar redes con capacidad de escalabilidad.

34. BIBLIOGRAFIA

Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1lhgCT9VCtl_pLtPD9

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

Vesga, J. (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>